IBM Cloud Application Performance Management, Private
Version 8.1.4 (updated July 2018)

Guide d'utilisation



SC43-4203-03

IBM Cloud Application Performance Management, Private
Version 8.1.4 (updated July 2018)

Guide d'utilisation



SC43-4203-03

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant dans la rubrique «Remarques», à la page 1199.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

© Copyright IBM France 2018. Tous droits réservés.

Cette édition s'applique à la version 8.1.4 d'IBM Cloud Application Performance Management, Base Private et d'IBM Cloud Application Performance Management, Advanced Private et à toutes les éditions et modifications ultérieures jusqu'à indication contraire dans les nouvelles éditions.

© Copyright IBM Corporation 2015, 2018.

Table des matières

Avis aux lecteurs canadiens xi

Chapitre 1. Nouveautés 1

Chapitre 2. Documentation au format PDF 29

Chapitre 3. Présentation du produit . . 31
Présentation de l'architecture 32
Interface utilisateur 34
Offres et modules complémentaires 35
Détails d'offre 37
Agents et collecteurs de données 40
Fonctions 40
Descriptions 44
Fonctions 59
Intégration 66
Documentation 68
Conventions utilisées dans la documentation . . 69

Chapitre 4. Configuration requise . . . 71
Eléments prérequis pour serveur Cloud APM . . . 72
Conseils pour la résolution des dépendances non satisfaites 83
Ports serveur Cloud APM 86
Ports par défaut utilisés par l'agent et les collecteurs de données 89
Configuration matérielle requise pour le serveur Cloud APM 92
Agents de surveillance IBM 96

Chapitre 5. Scénarios 97
Scénario : Surveillance d'IBM API Connect 97
Scénario : Surveillance de la Liste d'applications Java IBM 98
Surveillance de la Liste d'applications Java IBM 99
Ajout d'applications Web au Tableau de bord d'Application Performance 99
Association d'une Liste d'applications Java IBM à l'application Web 100
Affichage des résultats de la surveillance de la Liste d'applications Java IBM 101
Diagnostic des incidents de votre environnement 105
Scénario : Surveillance de la Pile d'intégration IBM 106
Surveillance de la Pile d'intégration IBM . . . 106
Ajout d'applications middleware au Tableau de bord d'Application Performance 107
Affichage des résultats de la surveillance de la Pile d'intégration IBM 108
Diagnostic des incidents de votre environnement 113

Chapitre 6. Instructions de téléchargement 115
Composants Cloud APM, Private 115
Packs d'extension 117
Produits regroupés avec Tivoli Monitoring . . . 117
Téléchargement depuis Passport Advantage . . . 118
Numéros de référence 118

Chapitre 7. Installation du serveur . . 125
Préparation de l'installation du serveur 125
Configuration du pare-feu pour les demandes entrantes sur le serveur 127
Définition des communications HTTP ou HTTPS 128
Connexion à un serveur Db2 distant. 129
Modification de l'authentification Db2 de server à server_encrypt 136
Passage d'une offre à une autre 138
Installation sur un système à l'aide d'un service d'annuaire externe. 138
Création d'utilisateurs Db2 avant la connexion à un serveur Db2 local 140
Téléchargement et installation du serveur 141
Désinstallation du serveur 148
Nettoyage des entrées Db2 149
Scanner de prérequis 149
Exécution manuelle du scanner de prérequis 150
Contournement de l'analyse des prérequis. . . 151
Installation d'une base de données MongoDB distante 152

Chapitre 8. Déploiement d'agents et de collecteurs de données. 155

Chapitre 9. Installation des agents 161
Configuration des images téléchargées 162
Installation des agents sur les systèmes AIX . . . 165
Préinstallation sur les systèmes AIX 165
Installation d'agents 167
Installation des agents sur les systèmes Linux . . 170
Préinstallation sur les systèmes Linux 171
Installation d'agents 175
Installation des agents sur les systèmes Windows 177
Préinstallation sur les systèmes Windows . . . 178
Installation d'agents 180
Installation des agents en tant qu'utilisateur non superutilisateur. 183
Sécurisation des fichiers d'installation de l'agent 184
Installation silencieuse des agents 185
Contournement de l'analyse des prérequis. . . . 186
Désinstallation de vos agents 187
Agent WebSphere Applications : Annulation de la configuration du collecteur de données . . . 189
Agent Node.js : Retrait du plug-in de surveillance 197

© Copyright IBM Corp. 2015, 2018

agent Microsoft .NET : Retrait du collecteur de données .NET 198

Chapitre 10. Configuration de votre environnement 201

Connectivité réseau 201
Communication sécurisée 201
Configuration des agents pour qu'ils communiquent via un proxy direct 201
Configuration des collecteurs de données pour qu'ils communiquent via un proxy direct . . . 202
Noms de systèmes gérés 204
Modification du nom de système géré de l'agent 207
Modification du nom d'hôte dans le nom de système géré 211
Configuration d'agents 212
Utilisation des commandes de l'agent 213
Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows 217
Page Configuration d'agent 218
Configuration des agents en tant qu'utilisateur non superutilisateur 219
Désactivation du démarrage automatique de l'agent sur les systèmes AIX et Linux 220
Connexion des agents à un autre serveur . . . 220
Configuration des certificats entre le serveur et les agents. 222
Configuration des collecteurs de données 232
Configuration de la passerelle sécurisée IBM Cloud 234
Reconnexion du collecteur de données au serveur Cloud APM 234
Exemple de fichier `manifest.yml` 237
Suppression de collecteurs de données de la console Cloud APM 237
Configuration de la surveillance d'Amazon EC2 238
Configuration de l'agent sur des systèmes Windows 239
Configuration de l'agent en répondant à des invites. 242
Configuration de l'agent en utilisant le fichier de réponses silencieux 243
Paramètres de configuration de l'agent Amazon EC2 244
Configuration de la surveillance d'AWS Elastic Load Balancer 245
Configuration de l'agent sur des systèmes Windows 246
Configuration de l'agent en répondant aux invites 248
Configuration de l'agent en utilisant le fichier de réponses silencieux 249
Paramètres de configuration de l'agent Amazon ELB 251
Configuration de la surveillance Azure Compute 251
Configuration de l'agent sur des systèmes Windows 252
Configuration de l'agent en répondant à des invites 255
Configuration de l'agent en utilisant le fichier de réponses silencieux 257
Paramètres de configuration de l'Agent Azure Compute 259
Configuration de la surveillance de Cassandra . . 261
Configuration de l'agent sur des systèmes Windows 262
Configuration de l'agent sur les systèmes Linux 262
Configuration de l'agent en utilisant le fichier de réponses silencieux 263
Paramètres de configuration de l'agent 264
Configuration de la surveillance de Cisco UCS . . 264
Configuration de l'agent sur des systèmes Windows 265
Configuration de l'agent en utilisant le fichier de réponses silencieux 266
Configuration de l'agent en répondant aux invites. 267
Paramètres de configuration pour l'agent . . . 268
Paramètres de configuration pour le fournisseur de données 268
Activation de la communication SSL avec les sources de données Cisco UCS 269
Augmentation de la taille de segment de mémoire Java 270
Configuration de la surveillance de Citrix Virtual Desktop Infrastructure 271
Activation des privilèges d'administrateur en lecture seule de Citrix 272
Configuration de l'agent sur des systèmes Windows 273
Configuration de l'agent en répondant à des invites. 276
Configuration de l'agent en utilisant le fichier de réponses silencieux 277
Paramètres de configuration de l'agent Citrix VDI 278
Activation de la surveillance des événements Windows et des mesures PowerShell 280
Configuration de la surveillance DataPower . . . 281
Configuration des dispositifs DataPower . . . 281
Configuration de l'agent DataPower 290
Configuration de la surveillance de Db2 294
Configuration de l'agent sur des systèmes Windows 295
Configuration de l'agent sur des systèmes Linux ou UNIX 296
Configuration de l'agent en utilisant le fichier de réponses silencieux 297
Octroi de privilèges pour l'affichage des mesures Db2 299
Configuration des variables d'environnement local 300
Prérequis pour la surveillance à distance . . . 304
Configuration de la surveillance de Hadoop . . . 305
Configuration de l'agent sur des systèmes Windows 306
Configuration de l'agent sur des systèmes Linux et AIX 309
Configuration de l'agent en utilisant le fichier de réponses silencieux 312

Configuration du tableau de bord pour visualiser des événements Hadoop 313
Attribution de droits aux utilisateurs non administrateurs. 313
Configuration de la surveillance de HMC Base . . 314
Configuration de la connexion SSH 316
Préparation du kit SDK pour HMC 317
Configuration du serveur de la console HMC pour la surveillance des entrées-sorties virtuelles 318
Activation de la surveillance de l'utilisation de l'UC et de la mémoire 318
Configuration de la surveillance de HTTP Server 319
module IBM HTTP Server Response Time . . . 321
Exemples de code pour l'agent HTTP Server 321
Configuration de la surveillance d'IBM Integration Bus 323
Configuration de l'agent IBM Integration Bus 324
Configuration d'IBM Integration Bus pour l'activation des données 328
Désactivation de la collecte de données d'image instantanée pour l'agent 332
Configuration du suivi des transactions pour l'agent IBM Integration Bus. 333
Spécification d'un nom de système géré unique pour agent IBM Integration Bus 333
Suppression de l'exit utilisateur KQIUserExit 334
Configuration de la surveillance d'IBM MQ Appliances 335
Configuration de l'agent en répondant à des invites. 336
Configuration de l'agent à l'aide du fichier de réponses silencieux 336
Paramètres de configuration de l'Agent MQ Appliance 337
Configuration de la surveillance d'InfoSphere DataStage 340
Configuration de l'agent sur des systèmes Windows. 340
Configuration de l'agent sur les systèmes Linux 341
Configuration de l'agent en utilisant le fichier de réponses silencieux 341
Paramètres de configuration de l'agent 342
Configuration d'Internet Service Monitor 344
Configuration d'Internet Service Monitoring par le biais de l'interface utilisateur 344
Configuration de l'agent sur des systèmes Windows. 415
Configuration de la surveillance de J2SE 418
Vérification du statut du suivi des transactions et de la collecte des données de diagnostic . . 421
Changement du statut du suivi des transactions et de la collecte des données de diagnostic . . 422
Configuration de la surveillance de JBoss 423
Activer les connexions au serveur JMX MBean 425
Ajout d'un utilisateur de gestion de serveur JBoss 426
Activation de la collecte des statistiques Web/HTTP 427
Configuration de l'agent sur des systèmes Windows. 428
Configuration de l'agent en répondant à des invites. 431
Configuration de l'agent en utilisant le fichier de réponses silencieux 432
Paramètres de configuration de l'agent JBoss 433
Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss 434
Configuration de la surveillance de Linux KVM 439
Création d'un utilisateur et attribution des droits nécessaires 439
Configuration des protocoles 440
Configuration d'une connexion au serveur RHEVM 444
Configuration d'une connexion au serveur RHEVH 446
Paramètres de configuration pour la connexion au serveur RHEVM 446
Paramètres de configuration pour la connexion au serveur RHEVH 448
Configuration de la surveillance de Microsoft Active Directory 450
Exécution de l'agent Microsoft Active Directory en tant qu'administrateur 450
Configuration des variables d'environnement local 451
Exécution de l'agent Microsoft Active Directory en tant qu'utilisateur non-administrateur . . . 452
Configuration de la surveillance de Microsoft Cluster Server 455
Création d'une ressource de cluster de service générique sur des systèmes Windows Server 2008 et 2012 456
Configuration de l'agent en utilisant le fichier de réponses silencieux 456
Modification du compte utilisateur 457
Configuration de la surveillance de Microsoft Exchange. 457
Création d'utilisateurs 458
Affectation des droits d'administrateur à l'utilisateur de Serveur Exchange 461
Attribution à l'utilisateur de Serveur Exchange des droits d'administrateur local 463
Configuration du Serveur Exchange pour l'accessibilité. 465
Configuration de l'agent pour qu'il s'exécute sous l'utilisateur de domaine 466
Configuration de l'agent en local 466
Configuration de l'agent en utilisant le fichier de réponses silencieux 470
Configuration des variables de l'environnement local pour l'agent 471
Configuration de la surveillance de Microsoft Hyper-V 471
Saisie de la stratégie de sécurité locale pour l'exécution de l'Agent de surveillance pour Microsoft Hyper-V Server sous Windows par un utilisateur non-administrateur 472
Octroi de droits de la stratégie de sécurité locale 473
Modification des droits DCOM 474
Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V 475

Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs Analyseur de performances 475
Configuration de la surveillance de Microsoft IIS 475
Configuration de l'agent sur des systèmes Windows 476
Configuration de l'agent en utilisant le fichier de réponses silencieux 477
Modification du compte utilisateur 478
Configuration de la surveillance Skype for Business Server (anciennement Microsoft Lync Server) . . . 478
Droits et droits d'accès d'un utilisateur non-administrateur 479
Configuration de l'agent sur des systèmes Windows 480
Configuration de l'agent en utilisant le fichier de réponses silencieux 481
Modification du compte utilisateur 482
Paramètres de configuration de l'agent 482
Configuration de la surveillance de Microsoft .NET 484
Droits nécessaires pour exécuter un agent à l'aide d'un compte local ou de domaine . . . 485
Enregistrement du collecteur de données . . . 485
Utilisation du module de temps de réponse IIS de l'agent .NET 486
Activation de la collecte des données de suivi des transactions et de diagnostic 488
Activation de la collecte des données de diagnostic à l'aide de la commande configdc . . 489
Activation du suivi des transactions dans l'environnement de coexistence d'agent 490
Activation des mises à jour de configuration 491
Optimisation des performances du collecteur de données 491
Configuration de la surveillance de Microsoft Office 365 494
Vérification de l'accessibilité des utilisateurs configurés 495
Configuration de l'agent sur des systèmes Windows 496
Configuration de l'agent en utilisant le fichier de réponses silencieux 497
Modification du compte utilisateur 498
Surveillance de la qualité de service Skype . . 498
Définition des variables d'environnement local 499
Configuration de la surveillance de Microsoft SharePoint Server 500
Modification du compte utilisateur 501
Exécution de Monitoring Agent for Microsoft SharePoint Server en tant qu'utilisateur non-administrateur 502
Droits de la stratégie de sécurité locale 503
Configuration de la surveillance de Microsoft SQL Server 504
Création d'un utilisateur et attribution des droits d'accès 505
Exécution en tant qu'utilisateur non-administrateur 509
Sélection des bases de données à surveiller . . 512
Définition des variables d'environnement local 521
Configuration de l'agent en utilisant le fichier de réponses silencieux 528
Exécution de l'agent dans un environnement cluster 528
Configuration de l'agent à l'aide de l'utilitaire Cluster 530
Configuration de plusieurs classements pour le fichier ERRORLOG 532
Configuration de la surveillance de MongoDB . . 533
Configuration de l'agent avec les paramètres par défaut 536
Configuration de l'agent en utilisant le fichier de réponses silencieux 536
Configuration de l'agent en répondant à des invites 538
Configuration de la surveillance de MySQL . . . 539
Configuration de l'agent sur des systèmes Windows 539
Configuration de l'agent sur des systèmes Linux 540
Configuration de l'agent en utilisant le fichier de réponses silencieux 541
Configuration de la surveillance de NetApp Storage 542
Téléchargement et installation du fichier JAR de NetApp Manageability SDK 543
Configuration de l'agent sur des systèmes Windows 543
Configuration de l'agent en utilisant le fichier de réponses silencieux 544
Configuration de l'agent en répondant à des invites 546
Paramètres de configuration du fournisseur de données 546
Paramètres de configuration d'OnCommand Unified Manager 547
Paramètres de configuration d'OnCommand API Service 548
Configuration de la surveillance de Node.js . . . 548
Configuration de l'Agent Node.js 549
Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud . . 555
Configuration du collecteur de données Node.js autonome pour les applications sur site . . . 561
Configuration de la surveillance d'OpenStack . . 567
Configuration de l'Agent OpenStack 568
Activation de la collecte des informations liées aux processus et des connexions SSH 570
Ajout des valeurs de configuration 571
Configuration de la surveillance d'Oracle Database 573
Configuration de l'agent sur des systèmes Windows 575
Configuration de l'agent en répondant à des invites 578
Configuration de l'agent en utilisant le fichier de réponses silencieux 582
Accord de privilèges à l'utilisateur de l'agent de base de données Oracle 586
Configuration de la surveillance du système d'exploitation 588
Exécution des agents de système d'exploitation en tant qu'utilisateur non superutilisateur . . . 588

Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation . 590
Configuration de la surveillance de PHP 617
Configuration de la surveillance PostgreSQL . . . 619
Configuration de l'agent sur des systèmes Windows 620
Configuration de l'agent sur les systèmes Linux 621
Configuration de l'agent en utilisant le fichier de réponses silencieux 622
Configuration de la surveillance Python 623
Configuration du collecteur de données Python pour les applications IBM Cloud 624
Configuration du collecteur de données Python pour les applications sur site 629
Configuration de la surveillance de RabbitMQ . . 635
Configuration de l'agent sur des systèmes Windows 635
Configuration de l'agent sur les systèmes Linux 636
Configuration de l'agent en utilisant le fichier de réponses silencieux 636
Paramètres de configuration de l'agent 637
Configuration de la surveillance des temps de réponse 638
Affichage des tableaux de bord de transactions 638
Response Time Monitoring Composants . . . 639
Planification de l'installation 640
Planification de la configuration 641
Injection JavaScript 642
Reconfiguration de la Response Time Monitoring sous Windows 643
Reconfiguration de la Response Time Monitoring sur AIX et Linux 644
Configuration à l'aide de la page Configuration d'agent 644
Ajout d'applications 646
Configuration du module IBM HTTP Server Response Time 647
Organigramme de l'Analyseur de paquets . . . 656
Personnalisation des valeurs de localisation Transaction utilisateur final 664
Suivi des applications Web supplémentaires . . 665
Spécification d'un nom de système géré unique pour l'Agent de surveillance des temps de réponse 668
Configuration de la surveillance de Ruby 669
Configuration de l'Agent Ruby 670
Configuration du collecteur de données Ruby pour les applications IBM Cloud 677
Configuration de la surveillance de SAP 681
Configuration de l'agent sur des systèmes Windows 682
Configuration de l'agent sur des systèmes Linux ou AIX 683
Configuration de l'agent en utilisant le fichier de réponses silencieux 683
Paramètres de configuration de l'agent 684
Importation du transport ABAP dans le système SAP 687
Suppression du transport ABAP du système SAP 693
Vérification de la configuration de l'agent . . . 694
Ajout du numéro de port de communication de base de données 698
Configuration de la surveillance de SAP HANA Database 699
Configuration de la surveillance de SAP NetWeaver Java Stack 701
Configuration de l'agent sur des systèmes Windows 702
Configuration de l'agent sur des systèmes Linux ou AIX 702
Configuration de l'agent en utilisant le fichier de réponses silencieux 703
Configuration du collecteur de données . . . 704
Activation de la collecte des données de suivi des transactions et de diagnostic 705
Suppression de la configuration du collecteur de données 707
Restauration de l'instance SAP NetWeaver Application Server 707
Paramètres de configuration de l'agent 708
Configuration de la surveillance de Siebel 708
Vérification du compte utilisateur Siebel . . . 709
Activation du paramètre "Per Component Statistics Monitoring". 710
Configuration de l'agent sur des systèmes Windows 711
Configuration de l'agent en répondant à des invites 715
Configuration de l'agent en utilisant le fichier de réponses silencieux 716
Paramètres de configuration de l'agent Siebel 717
Journaux de composant Siebel toujours surveillés 719
Configuration de la surveillance Sterling Connect Direct 719
Configuration de l'agent sur des systèmes Windows 720
Configuration de l'agent sur les systèmes Linux 720
Configuration de l'agent en utilisant le fichier de réponses silencieux 721
Paramètres de configuration de l'agent 721
Configuration de la surveillance Sterling File Gateway 722
Installation de l'API REST B2B 722
Configuration de l'Agent Sterling File Gateway sur des systèmes Windows 723
Configuration de l'Agent Sterling File Gateway sur les systèmes Linux 723
Configuration de l'Agent Sterling File Gateway à l'aide du fichier de réponses silencieux . . . 724
Configuration de variables d'environnement d'agent pour le fournisseur de données sous Linux 725
Configuration de variables d'environnement d'agent pour le fournisseur de données sous Windows 725
Variables d'environnement du fournisseur de données 726
Paramètres de configuration des détails de l'API B2B. 727

Paramètres de configuration des détails de la base de données 728
Paramètres de configuration de l'API Java . . . 728
Configuration de la surveillance de Sybase Server 728
Octroi de droits d'accès 729
Configuration de l'agent à l'aide de l'interface de ligne de commande 730
Configuration de l'agent à l'aide du fichier de réponses silencieux 732
Configuration de la surveillance de Synthetic Playback 734
Configuration de la surveillance de Tomcat . . . 735
Configuration de l'Agent Tomcat avec les paramètres par défaut 736
Configuration de l'agent sur des systèmes Windows 736
Configuration de l'Agent Tomcat sur les systèmes Linux 739
Configuration de l'Agent Tomcat à l'aide du fichier de réponses silencieux 740
Activation de la collecte des données de suivi des transactions et de diagnostic 741
Configuration de la surveillance de VMware VI 741
Définition de la taille et planification du déploiement de l'Agent VMware VI 743
Activation de la communication SSL avec les sources de données VMware VI 743
Configuration de l'agent sur des systèmes Windows 745
Configuration de l'agent en utilisant le fichier de réponses silencieux 746
Configuration de l'agent en répondant à des invites. 747
Paramètres de configuration de la source de données 747
Paramètres de configuration du fournisseur de données 748
Augmentation de la taille de segment de mémoire Java 749
Configuration de la surveillance de WebLogic . . 750
Configuration de l'agent sur des systèmes Windows 752
Configuration de l'agent en répondant à des invites 755
Configuration de l'agent en utilisant le fichier de réponses silencieux 756
Paramètres de configuration de l'Agent WebLogic. 758
Configuration du suivi des transactions pour l'Agent WebLogic 758
Configuration de votre Tableau de bord d'Application Performance pour l'affichage des données de suivi des transactions de l'Agent WebLogic. 765
Configuration de la surveillance des applications WebSphere 765
Configuration du collecteur de données pour l'Agent WebSphere Applications 766
Configuration du collecteur de données Liberty pour les applications sur site 813
Configuration du collecteur de données Liberty pour les applications IBM Cloud 845
Configuration de la surveillance de WebSphere Infrastructure Manager 852
Configuration de la surveillance de WebSphere MQ 853
ID utilisateur autorisés à exécuter l'agent . . . 854
Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données 855
Configuration de l'Agent WebSphere MQ . . . 857
Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente 860
Configuration du suivi des transactions pour l'Agent WebSphere MQ 862
Activation de la collecte de données pour l'historique à long terme de files d'attente et de canal 863
Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance 864
Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance . 866

Chapitre 11. Intégration à d'autres produits et composants 871

Intégration à IBM Tivoli Monitoring V6.3 871
Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring 872
Passerelle hybride 875
Tivoli Data Warehouse pour le rapport de l'historique 888
Intégration à OMEGAMON 905
Intégration à Netcool/OMNIbus 905
Configuration de l'intégration pour Netcool/OMNIbus 905
Intégration à Operations Analytics - Log Analysis 907
Intégration à Operations Analytics - Predictive Insights 908
Intégration à Alert Notification 908
Intégration à IBM Cloud. 910
Surveillance d'IBM Cloud Private. 911
Surveillance de vos conteneurs IBM Cloud Private 911
Surveillance de vos applications IBM Cloud Private 915
Intégration à Tivoli Common Reporting 917
Téléchargement et installation de Tivoli Common Reporting 918
Configuration d'une connexion ODBC 918
Configuration de l'image d'installation des rapports 919
Installation des rapports. 920
Configuration de la connexion unique avec Tivoli Common Reporting 922
Intégration à Dashboard Application Services Hub 925
Configuration de la connexion unique avec Jazz for Service Management version 1.1.2.0 ou ultérieure. 926
Configuration de l'intégration de console . . . 929
Connexion au fournisseur de données IBM Cloud Application Performance Management . 929

Création de tableaux de bord personnalisés avec des données IBM Cloud Application Performance Management 930
Intégration à LDAP 931
Ajout du certificat du serveur LDAP 931
Mise à jour du fichier de registre LDAP . . . 932
Intégration à IBM Agent Builder 939

Chapitre 12. Mise à niveau 941
Mise à niveau de votre serveur 941
Installation de MongoDB V3.2.12 sur votre système distant 942
Mise à niveau du serveur sur le même système 945
Mise à niveau du serveur côte à côte 955
Mise à niveau du serveur connecté à un serveur Db2 distant 967
Mise à niveau de vos agents 975
Conservation des changements apportés à la configuration des agents. 977
Agents sous AIX : arrêt de l'agent et exécution de **slibclean** avant la mise à niveau 978
agent HMC Base sous AIX : Arrêt de l'agent en tant qu'utilisateur non superutilisateur et exécution de **slibclean** avant la mise à niveau . 979
Agent Node.js : suppression des plug-in de collecteur de données avant la mise à niveau. . 979
Agent Response Time Monitoring : mise à niveau de module IBM HTTP Server Response Time 980
agent Microsoft .NET : suppression du collecteur de données .NET avant la mise à niveau. 980
Agent OpenStack : reconfiguration des instances de l'agent pour utiliser OpenStack Identity API v3 981
Agent Ruby : suppression des plug-in de collecteur de données avant la mise à niveau. . 981
Agent WebSphere Applications : migration du collecteur de données 982
Agent Tomcat : mise à niveau de TEMA Core Framework sous Windows 986
Mise à niveau de vos collecteurs de données . . . 986

Chapitre 13. Gestion 989
Démarrage de la console Cloud APM 989
Seuils et groupes de ressources 990
Informations de référence 990
Gestionnaire de groupes de ressources 995
Tutoriel : Définition d'un seuil. 998
Tutoriel : Définition d'un seuil pour exécuter une commande sur la ressource gérée 1001
Gestionnaire de seuils 1002
Personnalisation d'un événement à transmettre à un récepteur EIF 1007
Utilisation de l'API Resource Group Management Service 1014
Utilisation de l'API Threshold Management Service 1017
Gestion des accès utilisateur 1020
Rôles et droits. 1021
Configuration de la consignation d'audit pour l'activité de contrôle d'accès basé sur les rôles . 1028
Configuration des certificats pour la console Cloud APM 1030
Accès et utilisation de l'API Role-Based Access Control Service 1037
Administration de vos agents 1039
Démarrage d'agents en tant qu'utilisateur non superutilisateur 1039
Gestion des valeurs de conservation des données d'historique 1040
Seuils d'événement pour la surveillance des transactions 1045
Gestion des événements d'agent de système d'exploitation 1049
Gestion des transactions et des événements synthétiques 1058
Instructions pour la maximisation des performances du serveur et des agents dans le cadre de la surveillance des fichiers journaux . 1071
Administration des composants serveur 1075
Mots de passe et ID utilisateur des composants 1075
Modification de la version et de l'emplacement du serveur Db2 ou des noms de base de données après l'installation du serveur Cloud APM 1078
Démarrage, arrêt et vérification du statut des composants serveur 1090
Gestion de la taille du segment de mémoire Java maximale et du pool de mémoire tampon Db2 1093
Modification de l'adresse IP et du nom d'hôte du serveur 1096
Configuration du protocole de communications pour les agents de serveur 1097
Basculement vers une base de données MongoDB locale 1099
Conservation des transactions de middleware 1100
Sauvegarde et restauration de composants . . 1101
Exploration des API 1115
Ajustement de la valeur de délai de la console 1115
Configuration avancée 1117
E-mail d'événement 1122

Chapitre 14. Utilisation des tableaux de bord 1125
Toutes mes applications - Tableau de bord d'Application Performance 1125
Recherche dans les fichiers journaux 1127
Application - Tableau de bord d'Application Performance 1128
Manipulation du widget Agréger une topologie de transaction 1132
Groupe et Instance - Tableau de bord d'Application Performance 1133
Edition des widgets de groupe du tableau de bord Composants. 1137
Ajustement et comparaison de mesures dans le temps 1138
Affichage et gestion de graphiques et tableaux personnalisés 1139

Gestion des applications 1145
Ajout d'une application. 1146
Edition d'une application 1149
Suppression d'une application 1150
Affichage et suppression des agents en ligne 1151
Statut de l'événement 1156
Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights 1159
Vues personnalisées 1160
Création et gestion de pages personnalisées 1160
Affichage de pages personnalisées 1167
Utilitaires de tableau de bord. 1170
Copie de l'URL du tableau de bord. 1170
Définition d'une trace 1170
Verrouillage de la console Cloud APM . . . 1172
Rapports 1172
Rapports de l'Agent de surveillance des temps de réponse 1173
Génération de rapports sur l'Agent Synthetic Playback 1177
Rapports de l'Agent WebSphere Applications 1182

Chapitre 15. IBM Cloud Application Business Insights 1187

Chapitre 16. Traitement des incidents et support 1189
Collecte des journaux du serveur Cloud APM pour le support IBM. 1189
Collecte des journaux d'agent de surveillance pour le support IBM 1194

Fonctions d'accessibilité 1197

Remarques 1199
Marques. 1201
Dispositions relatives à la documentation du produit 1201
Déclaration IBM de confidentialité sur Internet 1202

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

© Copyright IBM Corp. 2015, 2018

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Chapitre 1. Nouveautés

De nouvelles fonctions, fonctionnalités et offres sont disponibles dans la dernière édition.

- Pour obtenir la description de l'édition actuelle, voir «Nouveautés pour l'édition Septembre 2018 de la version 8.1.4»
- Pour une description d'une version antérieure, voir «Nouveautés de l'édition de juillet 2018 pour la version 8.1.4», à la page 2, «Nouveautés de l'édition d'avril 2018 pour la version 8.1.4», à la page 4, «Nouveautés pour l'édition Février 2018 de la version 8.1.4», à la page 6, «Nouveautés de la version 8.1.4 actualisée en décembre 2017», à la page 7 «Nouveautés de la version 8.1.4», à la page 9 ou «Versions précédentes», à la page 21
- Pour plus d'informations sur la version de l'agent dans chaque édition ou actualisation, voir Agent version in Cloud APM, Private releases

Nouveautés pour l'édition Septembre 2018 de la version 8.1.4

Améliorations au niveau des agents

Monitoring Agent for Db2
L'agent Db2 prend maintenant en charge le système d'exploitation Power Linux Big Endian.

Monitoring Agent for Hadoop

- L'agent Hadoop surveille maintenant l'état de deux autres services : SmartSense et Druid.
- L'agent Hadoop prend maintenant en charge Hortonworks Data Platform (HDP) 3.0.0.

Internet Service MonitoringAgent
Les fonctionnalités d'édition de l'agent Internet Service Monitoring sont améliorées. Tous les moniteurs qui possèdent des paramètres configurables peuvent être modifiés.

Monitoring Agent for MySQL
L'agent MySQL prend maintenant en charge la surveillance de MySQL v8.0.11.

Monitoring Agent for NetApp Storage
L'agent NetApp Storage est amélioré à l'aide des fonctions suivantes :

- Un nouveau widget, Overall Events Summary, est ajouté à la page Instance de stockage NetApp. Il affiche le nombre total d'événements. Vous pouvez afficher tous les événements survenus dans l'environnement, indépendamment de leur gravité ou de leur objet en cliquant sur la barre d'état, sous le nom Total Events.

  De plus, une colonne Statut de l'événement est ajoutée dans chaque table d'objets. Elle affiche l'état des événements, classés en fonction de l'heure et du niveau de gravité.

  La page Instance de stockage NetApp affiche maintenant la table Events Summary au lieu d'un graphique.
- La page Aggregate Details est mise à jour pour afficher les périphériques connexes qui sont associés à l'agrégat sélectionné.

Monitoring Agent for SAP Applications
Ajout de la prise en charge de SAP NW RFC SDK 750.

Monitoring Agent for SAP HANA Database
Ajout de deux nouvelles fonctions :

- La base de données SAP HANA peut être surveillée en mode veille.
- Agent SAP HANA Database prend en charge la plateforme Big Endian pour Power System.

© Copyright IBM Corp. 2015, 2018

Monitoring Agent for VMware VI

- La surveillance de **HostVFlashManager** est maintenant prise en charge
- Le tableau de bord du serveur ESX affiche maintenant le nombre de machines virtuelles dont l'utilisation de l'UC est à l'état Critique, Avertissement et Normal.

Nouvel agent disponible

Monitoring Agent for MQ Appliance

L'agent MQ Appliance fournit des informations de surveillance relatives au niveau de MQ Appliances, telles que des informations récapitulatives sur l'UC, la mémoire, le stockage, les capteurs et les gestionnaires de files d'attente.

Nouveautés de l'édition de juillet 2018 pour la version 8.1.4

Correctif temporaire 6 du serveur Cloud APM 8.1.4.0

Après avoir appliqué le correctif temporaire 6 du serveur Cloud APM 8.1.4.0, vous pouvez :

- Modifier les noms des bases de données Db2 du serveur Cloud APM sur le serveur Db2 distant.
- Modifier le numéro de port, le nom d'hôte ou l'adresse IP du serveur Db2 distant.
- Déplacer les bases de données Db2 du serveur Cloud APM vers un autre système ou vers un autre utilisateur d'instance Db2.

Nouveaux agents disponibles

Internet Service Monitoring

Internet Service Monitoring permet de déterminer si un service particulier fonctionne de manière adéquate, d'identifier les zones problématiques et de générer un rapport sur les performances du service mesurées par rapport aux exigences des contrats de niveau de service (SLA). Internet Service Monitoring fonctionne par émulation des actions d'un utilisateur réel. Il interroge ou teste régulièrement les services Internet pour vérifier leur statut et leurs performances.

Monitoring Agent for Sybase Server

L'agent Sybase offre un point central de gestion des bases de données réparties. Il collecte les informations requises pour que les administrateur de base de données et système puissent examiner les performances du système Sybase Server, détecter rapidement les problèmes et les empêcher.

Améliorations au niveau des agents

Monitoring Agent for Hadoop

- Ajout de la prise en charge de la surveillance des services Hadoop, tels que Mahout, Atlas et Falcon.
- Ajout de la prise en charge de la surveillance de l'offre Hadoop : Cloudera CDH 5.13.
- Ajout de la prise en charge de la surveillance de l'offre Hadoop : Hortonworks HDP 2.6.4.

Monitoring Agent for HMC Base

HMC V8 R8.7.0 est désormais pris en charge.

Monitoring Agent for HTTP Server

Le support d'Apache HTTP Server sous Windows 64 bits a été ajouté.

Monitoring Agent for Microsoft .NET

L'Monitoring Agent for Microsoft .NET a été étendu comme suit :

- Le module de temps de réponse IIS surveille maintenant la répartition des temps de rendu et des sous-transactions via l'injection JavaScript pour les formulaires Web ASP.NET (pages .aspx) et les vues MVC Razor ASP.NET, qui remplissent les conditions suivantes :
  - La page respecte les normes HTML W3C.
  - Les en-têtes de réponse contiennent `Content-Type: text/html, application/xml,application/json`.
  - Le contenu de réponse inclut l'élément *<head>*.
- L'agent .NET télécharge les données d'analyse approfondie sur le service DQE (Diagnostic Query Engine), sur le serveur APM. Le tableau de bord d'analyse approfondie du service DQE charge et affiche rapidement les données.
- La nouvelle situation NET_Slow_IIS_Request_Crit est ajoutée ; elle est déclenchée si le widget Slow Top 10 contient des demandes dont le temps de réponse est supérieur à 500 millisecondes.
- L'outil de filtrage sélectif est mis à jour avec la zone de recherche pour rechercher un pool d'applications dans la liste des pools d'applications.
- L'utilitaire **ProcListCaller** est ajouté pour fournir la liste des processus ayant chargé le profileur CLR de l'agent .NET (`CorProfLog.dll`).

Monitoring Agent for Microsoft SQL Server

- L'agent Microsoft SQL Server prend désormais en charge plusieurs classements dans l'analyse syntaxique `ERRORLOG` en fonction des paramètres de classement du fichier `koqErrConfig.ini`. Si le fichier `koqErrConfig.ini` ne contient pas de paramètres de classement valides, vous ne pourrez voir que le message d'erreur anglais par défaut dont le niveau de gravité est supérieur au niveau de gravité par défaut (s'il en existe un). Le niveau de gravité par défaut est de 17. Tous les classements qui se trouvent dans le fichier `koqErrConfig.ini` sont pris en compte lors de l'analyse syntaxique du fichier `ERRORLOG`. Par conséquent, les classements en cours d'utilisation doivent être ajoutés dans le fichier `koqErrConfig.ini`. L'analyse syntaxique du fichier `ERRORLOG` étant sensible à la casse, vous devez vous assurer que les valeurs des mots clés de classement dans le fichier `koqErrConfig.ini` sont identiques à celles du fichier `ERRORLOG` ou du fichier `koqErrConfigSample.ini` de référence. Notez que les modifications apportées au fichier `koqErrConfig.ini` ne sont pas conservées lors de la mise à niveau de l'agent ; vous devez effectuer une sauvegarde au préalable.
- L'agent fournit également l'utilitaire **koqVerifyPermissions.exe** pour vérifier si un utilisateur SQL Server existant dispose de droit suffisants pour surveiller Microsoft SQL Server. Si un utilisateur SQL Server existant ne dispose pas de droits suffisants, vous pouvez utiliser l'utilitaire **permissions.cmd** comme autre moyen d'octroyer les droits minimaux à un utilisateur SQL Server existant pour la collecte des données.

Monitoring Agent for NetApp Storage

L'Monitoring Agent for NetApp Storage a été étendu comme suit :

- La nouvelle page Composant a été ajoutée pour afficher les détails de l'état de connexion de l'agent que le fournisseur de données soit actif ou inactif, avec l'adresse IP des sources de données surveillées. La barre de statut individuelle représente le nombre de noeuds, d'agrégats, de volumes et de disques à l'état critique, normal, avertissement ou inconnu.
- La nouvelle page Instance de stockage NetApp a été ajoutée pour mettre en évidence les principales propriétés des clusters, agrégats, volumes, disques et serveurs virtuels. Elle affiche également un graphique Events Summary qui indique le nombre d'événements correspondant à chaque entité de l'environnement. Par exemple, si 12 volumes sont configurés et que chacun comporte deux événements de niveau de gravité Critique, le diagramme Event Summary illustre le nombre total d'événements

survenus dans tous les volumes disponibles dans un environnement. Dans ce cas, le diagramme affiche une barre comportant 24 événements critiques comparés au volume sous forme d'entité tracée sur l'axe des X.

- La page Node Details a été mise à jour pour afficher les détails des ports réseau.
- La page Volume Detail a été mise à jour pour afficher les détails des miroirs des instantanés associés et le nombre d'unités logiques de chaque volume sélectionné.
- La page vServers Details a été mise à jour pour afficher les informations sur les interfaces logiques du réseau.

Monitoring Agent for Tomcat

Le serveur Tomcat V9.0.5 est désormais pris en charge.

Monitoring Agent for WebSphere MQ

La surveillance éloignée est prise en charge. Deux paramètres de configuration ont été ajoutés pour que l'agent puisse collecter les données de surveillance d'un gestionnaire de files d'attente éloignées. Toutefois, ces paramètres de configuration n'ont aucun impact sur un gestionnaire de files d'attente locales. Si vous souhaitez configurer l'agent pour qu'il surveille un gestionnaire de files d'attente locales, vous pouvez appuyer sur Entrée pour ignorer la spécification de ces paramètres.

Pour plus d'informations sur la configuration de l'agent, voir «Configuration de l'Agent WebSphere MQ», à la page 857.

Amélioration de la personnalisation de l'emplacement de la fonction d'intégration d'événements

Vous pouvez désormais ajouter plusieurs valeurs d'attribut et valeurs littérales à l'emplacement de la fonction d'intégration d'événements. Ainsi, par exemple, au lieu d'un message `Disk free percent is` **`Disk_Free_Percent`** pour un seuil qui vérifie si l'espace disque disponible est faible, vous pourriez avoir le message `Disk free percent is` **`Disk_Free_Percent`** `and inodes free percent is` **`Inodes_Free_Percent`**. Le message transmis peut se présenter comme suit : `Disk free percent is 13 and inodes free percent is 9`. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1007.

IBM Cloud Application Business Insights

Vous pouvez utiliser l'application IBM Cloud Application Business Insights autonome qui promeut la démocratisation des données pour les utilisateurs professionnels et les PME. Elle offre un outil de visualisation et d'exploration des données avancé et puissant qui fonctionne au delà de la génération de rapports classique.

Actuellement, l'outil Dashboard Designer dispose de connecteurs par défaut aux sources de données des agents Cloud APM et IBM® Tivoli Monitoring pour extraire et présenter des informations sur vos tableaux de bord personnalisés. Vous pouvez également connecter un grand nombre de bases de données relationnelles pour créer des tableaux de bord.

Pour plus d'informations, voir la documentation IBM Cloud Application Business Insights sur l'IBM Knowledge Center.

Nouveautés de l'édition d'avril 2018 pour la version 8.1.4

Nouvel agent disponible

Monitoring Agent for AWS Elastic Load Balancer

L'agent Amazon ELB permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos équilibreurs de charge élastiques AWS. L'agent affiche un ensemble complet de mesures pour chaque type d'équilibreur de charge, application, réseau et classique, qui vous aident à prendre des décisions avisées concernant votre environnement AWS Elastic Load Balancer.

Améliorations au niveau des agents

Agent de surveillance des temps de réponse
Le module IBM HTTP Server Response Time prend désormais en charge IBM HTTP Server version 7, 8 et 9 sous Windows.

Monitoring Agent for Node.js
Par défaut, les informations sensibles de l'utilisateur, telles que les cookies, les contextes de demande HTTP et les contextes de requête de base de données, ne sont plus collectées par le collecteur de données Node.js. Vous pouvez modifier ce comportement par défaut en spécifiant la nouvelle variable d'environnement, *SECURITY_OFF*.

Monitoring Agent for Amazon EC2
Le nom du composant reflète désormais le nom de l'agent.

La conservation étendue des données est désormais prise en charge.

Monitoring Agent for WebLogic
Le suivi des transactions et le diagnostic approfondi sont activés sous AIX. Auparavant, ces fonctions n'étaient activées que sous Linux et Windows.

L'analyse détaillée Récapitulatif des demandes pour les servlets implémentés avec des annotations pour le suivi des transactions et le diagnostic approfondi a été améliorée.

Monitoring Agent for Skype for Business Server
Prise en charge de Windows Server 2016.

Monitoring Agent for Sterling File Gateway
Par défaut, l'agent extrait les événements relatifs au transfert de fichier ayant échoué. Vous pouvez modifier ce comportement par défaut en spécifiant la valeur appropriée pour la nouvelle variable d'environnement **KFG_ALL_FGEVENTS**.

Monitoring Agent for Sterling Connect Direct
La fonction de consignation de l'agent a été améliorée. Pour plus d'informations, voir la section de traitement des incidents.

Améliorations apportées au collecteur de données

collecteur de données Node.js
Par défaut, les informations sensibles de l'utilisateur, telles que les cookies, les contextes de demande HTTP et les contextes de requête de base de données, ne sont plus collectées par le collecteur de données Node.js. Vous pouvez modifier ce comportement par défaut en spécifiant la nouvelle variable d'environnement, *SECURITY_OFF*.

A faire : Pour obtenir cette amélioration, vous devez télécharger et appliquer le correctif temporaire 1 du collecteur de données Node.js d'IBM Cloud Application Performance Management à partir d'IBM Fix Central. Pour plus d'informations, voir Interim Fix 1 Readme File.

collecteur de données J2SE
La reconnaissance automatique de la classe de point d'entrée (classe Main) et du nom d'alias de l'application J2SE est désormais prise en charge.

Le suivi des transactions et le diagnostic approfondi peuvent être activés et désactivés en local à l'aide des scripts de configuration.

Améliorations apportées à la documentation
Une page Web a été créée dans Application Performance Management Developer Center pour vous aider à trouver le niveau de l'agent dans chaque révision ou édition. Pour plus d'informations, voir Agent version in Cloud APM, Private releases.

Le tableau Fonctions de l'agent et du collecteur de données dans chaque offre a été simplifié pour une meilleure lisibilité. Pour plus d'informations, voir «Fonctions», à la page 40.

Nouveautés pour l'édition Février 2018 de la version 8.1.4

Nouvel agent disponible

Monitoring Agent for Azure Compute

L'Agent Azure Compute permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Azure Compute. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement Azure Compute. Ces métriques incluent l'utilisation de l'UC, l'utilisation du réseau et les performances du disque.

Monitoring Agent for Sterling Connect Direct

Vous pouvez utiliser l'Agent Sterling Connect Direct pour surveiller la santé et les performances du serveur Sterling Connect Direct. Il surveille les fonctions du serveur Sterling Connect Direct, telles que les activités de transfert de fichiers, les processus planifiés et les processus de mise en attente et de file d'attente. Cet agent multi-instance prend en charge la surveillance à distance.

Monitoring Agent for Sterling File Gateway

L'Agent Sterling File Gateway surveille l'application Sterling File Gateway, utilisée pour transférer des fichiers entre les partenaires internes et externes à l'aide de différents protocoles, différentes conventions de dénomination de fichier et différents formats de fichier. Il prend également en charge la fonction de surveillance à distance.

Améliorations au niveau des agents

Monitoring Agent for DataPower
Le suivi des transactions entre l'Agent WebSphere MQ et l'agent DataPower est pris en charge.

Monitoring Agent for Db2
Ajout de la prise en charge de la surveillance à distance.

Monitoring Agent for Hadoop
Ajout de la prise en charge de la surveillance du statut des services Hadoop, tels que HBase, MapReduce2, Tez et Ranger.

La prise en charge de la surveillance de l'offre Hadoop : Cloudera CDH 5.12 a été ajoutée.

Monitoring Agent for InfoSphere DataStage
Ajout de la prise en charge de MS SQL en tant que référentiel de métadonnées.

La prise en charge du système d'exploitation Windows a été ajoutée.

Monitoring Agent for Tomcat
Prise en charge du suivi des transactions et de l'analyse approfondie pour PLinux en mettant à niveau l'infrastructure de l'agent avec le correctif 8.1.4.0-IBM-APM-SERVER-IF0001.

Monitoring Agent for SAP Applications
Amélioration de la fonction CCMS : automatisation de la suppression du fichier `idx`. Cette automatisation fonctionne uniquement lorsque le système SAP est redémarré.

Monitoring Agent for SAP NetWeaver Java™ Stack
Ajout de la prise en charge des applications Spring Boot.

Monitoring Agent for Microsoft .NET
La prise en charge des transactions d'utilisateur final à l'aide du module de temps de réponse IIS a été ajoutée.

Monitoring Agent for Skype for Business Server
Le nom de l'agent Monitoring Agent for Microsoft Lync Server est modifié en Monitoring Agent for Skype for Business Server.

Monitoring Agent for Linux KVM
Ajout de la prise en charge de RHEV-M 4.x.

Monitoring Agent for Linux OS
L'intervalle de transfert de mémoire est redéfini sur 1 minute.

L'adresse IP associée à l'interface réseau s'affiche sur le tableau de bord du système d'exploitation Linux et sur le widget System Information.

Monitoring Agent for UNIX OS
L'intervalle de transfert de mémoire est redéfini sur 1 minute.

Nouveautés de la version 8.1.4 actualisée en décembre 2017

Nouvel agent disponible

Monitoring Agent for InfoSphere DataStage

L'Agent DataStage permet de surveiller la santé et les performances des ressources du serveur DataStage, telles que les services de moteur, les systèmes de moteur, l'activité des tâches,le statut d'exécution des tâches et les détails d'exécution des tâches. Cet agent prend en charge la surveillance à distance.

Améliorations au niveau des agents

Monitoring Agent for Hadoop

Ajout de la prise en charge de la surveillance d'un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO, qui utilise le centre de distribution de clés (KDC) Active Directory.

Ajout de la prise en charge des tests de connexion aux hôtes d'un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO, qui utilise le centre de distribution de clés (KDC) MIT ou Active Directory.

Ajout de la prise en charge de la surveillance des offres Hadoop suivantes : Cloudera CDH 5.10 et CDH 5.11.

Ajout de la prise en charge de la surveillance du statut des services Hadoop tels que Flume, Kafka, Titan, Spark, Knox, Pig, Slider et Solr.

Monitoring Agent for HTTP Server
Ajout de la prise en charge de IBM HTTP Server et d'Apache HTTP Server Windows 32 bits.

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Ajout de la prise en charge d'Oracle HTTP Server sous Linux for System.

Monitoring Agent for IBM Integration Bus
Ajout de la prise en charge de Linux for Power Systems (Little Endian).

A faire : Pour bénéficier de la prise en charge du suivi des transactions sous Linux for Power Systems (Little Endian), vous devez, avant de démarrer l'agent, télécharger et appliquer le correctif temporaire 01 de IBM Cloud Application Performance Management 8.1.4 Core Framework à partir de Fix Central.

Monitoring Agent for Microsoft .NET
Ajout de la prise en charge de la surveillance d'ODP.NET.

Ajout des détails de trace de la méthode HttpWebRequest.GetResponse().

Monitoring Agent for Microsoft SQL Server

Ajout de la prise en charge de la tolérance pour SQL Server 2017.

Ajout de la prise en charge de la fonction Always On pour l'édition SQL Server destinée aux développeurs.

Monitoring Agent for MySQL

Ajout de la prise en charge de la tolérance des tables de schéma d'informations migrées vers le schéma de performances.

Ajout de la prise en charge des tables obsolètes du schéma d'informations via le schéma de performances.

Monitoring Agent for Microsoft Internet Information Services

Ajout de la prise en charge de la surveillance des sites Web FTP.

Monitoring Agent for MongoDB

Ajout de la prise en charge de la surveillance à distance.

Ajout de la prise en charge de la surveillance du moteur de stockage en mémoire.

Monitoring Agent for OpenStack

Ajout de la prise en charge de l'API OpenStack Authentication version 3.

Monitoring Agent for Oracle Database

La version d'agent est passée à la version 8.0.

Ajout du paramètre de configuration **`Oracle JDBC jar file`** et suppression des paramètres de configuration **`Oracle Home Directory`** et **`Oracle Instant Client Installation Directory`**.

Monitoring Agent for PostgreSQL

Ajout de la prise en charge de la surveillance à distance.

Monitoring Agent for SAP Applications

Ajout de la prise en charge de la communication SNC.

Ajout d'une nouvelle situation pour l'arrêt des systèmes SAP.

Monitoring Agent for SAP NetWeaver Java Stack

Ajout de la fonction de restauration de l'instance SAP NetWeaver Application Server.

Monitoring Agent for Tomcat

Ajout de la prise en charge de Linux for Power Systems (Little Endian) (surveillance des ressources uniquement).

Monitoring Agent for VMware VI

Ajout des paramètres Résumé de réseau et Nombre de disques sur la page de présentation du serveur ESX Server.

Ajout du widget de groupe Evénements sur la page Récapitulatif de cluster.

Monitoring Agent for WebSphere Applications

Ajout de la prise en charge du suivi des transactions pour Linux for Power Systems (Little Endian) et Linux for System z.

A faire : Pour bénéficier de la prise en charge du suivi des transactions sous Linux for Power Systems (Little Endian) et Linux for System z, procédez comme suit :

1. Téléchargez l'image d'installation de l'agent.
2. Installez l'Agent WebSphere Applications.
3. Téléchargez le correctif temporaire 2 pour l'Agent WebSphere Applications à partir de Fix Central.

4. Suivez les instructions indiquées dans le fichier Readme du correctif temporaire pour l'appliquer.

Monitoring Agent for WebSphere MQ

Ajout du widget de groupe Statut de service MQ qui fournit des détails sur le service MQ.

Ajout de la prise en charge de Linux for Power Systems (Little Endian).

A faire : Pour bénéficier de la prise en charge du suivi des transactions sous Linux for Power Systems (Little Endian), vous devez, avant de démarrer l'agent, télécharger et appliquer le correctif temporaire 01 de IBM Cloud Application Performance Management 8.1.4 Core Framework à partir de Fix Central.

Agent de surveillance des temps de réponse

Ajout de la prise en charge de IBM HTTP Server et d'Apache HTTP Server Windows 32 bits.

Améliorations apportées au collecteur de données

collecteur de données Liberty

Modification du nom de système géré (MSN) enregistré par le collecteur de données Liberty afin de refléter le nom d'hôte et le nom du serveur Liberty. Le nouveau MSN de ce collecteur de données est `BI:`*`nomserveur_nomhôte_md5`*`:BLP`, où *md5* est le GUID de l'application locale basé sur MD5. La longueur de *nomserveur_nomhôte_md5* est de 25 caractères.

A faire : Pour obtenir cette amélioration, vous devez télécharger et appliquer le correctif intermédiaire 1 du collecteur de données IBM Cloud Application Performance Management Liberty à partir de Fix Central.

collecteur de données J2SE

Ajout de la prise en charge du suivi des transactions des applications J2SE.

Améliorations apportées à la documentation

Ajout d'informations sur les ports par défaut utilisés par les agents et les collecteurs de données afin de vous aider à préparer l'environnement. Voir «Ports par défaut utilisés par l'agent et les collecteurs de données», à la page 89.

Ajout d'informations sur les noms de système gérés (MSN) des agents Cloud APM. Des instructions sur la procédure de modification de la chaîne de nom d'hôte du MSN sont également fournies. Voir «Noms de systèmes gérés», à la page 204.

Ajout d'informations sur l'exécution d'un agent en tant qu'utilisateur non-administrateur ou sur les droits requis à cet effet dans les rubriques de configuration associées aux agents suivants :

- agent Microsoft .NET
- agent Microsoft Active Directory
- agent Microsoft Exchange Server
- Agent Skype for Business Server
- agent Microsoft SharePoint Server
- agent Microsoft SQL Server
- Agent Tomcat

Nouveautés de la version 8.1.4

Application Performance Management Developer Center

L'APM Developer Center est un emplacement central à partir duquel vous pouvez accéder à des ressources pour les produits APM : blogues, vidéos, documentation, support, événements, IBM

Marketplace, et d'autres ressources. Le menu **Aide**de la console Cloud APM contient un lien pratique vers l'Application Performance Management Developer Center.

Nouvelle stratégie de marque et simplification du produit

Les offres IBM Performance Management sur site ont été rebaptisées et consolidées en IBM Cloud Application Performance Management, Base Private et IBM Cloud Application Performance Management, Advanced Private, comme illustré dans le tableau.

Nom de l'offre : édition V8.1.3 et éditions antérieures	Nom de l'offre : édition V8.1.4 et éditions ultérieures
Surveillance	Cloud APM, Base Private
Application Performance Management Advanced	Cloud APM, Advanced Private

Certains noms de composant ont également été modifiés : la console Cloud APM et le serveur Cloud APM étaient appelés console Performance Management et serveur Performance Management dans les versions antérieures.

Certaines extensions de produit ont été consolidées et renommées :

Nom de l'extension : édition V8.1.3 et éditions antérieures	Nom de l'extension : édition V8.1.4 et éditions ultérieures
Base Extension Pack (agent Hadoop)	Base Extension Pack (ajout du nouvel agent Cassandra et du nouvel agent Microsoft Office 365)
Advanced Extension Pack (Agent SAP HANA Database et Agent SAP NetWeaver Java Stack)	Advanced Extension Pack (ajout du nouvel agent RabbitMQ)

Surveillance d'IBM API Connect

Les agents et les collecteurs de données Cloud APM prennent maintenant en charge la surveillance de l'environnement IBM API Connect. Vous pouvez déployer les agents et les collecteurs de données correspondants pour obtenir un aperçu de la santé et des performances des composants de votre environnement. Les données de suivi des transactions sont également disponibles, en plus des données de surveillance et de diagnostic approfondi des transactions, ce qui vous permet d'afficher les informations de topologie concernant votre environnement IBM API Connect. Pour plus d'informations, voir «Scénario : Surveillance d'IBM API Connect», à la page 97.

Surveillance de la IBM Cloud Private

Vous pouvez surveiller à la fois vos conteneurs Cloud Private et vos applications Cloud Private basées sur Liberty à partir de la console Cloud APM. Pour plus d'informations, voir «Surveillance d'IBM Cloud Private», à la page 911.

Prise en charge de systèmes d'exploitation

Linux for System z

Ajout de la prise en charge de Linux for System z pour les agents de surveillance suivants : Linux OS, WebSphere Application, Db2, WebSphere MQ, IBM Integration Bus, Tomcat et Response Time Monitoring.

Linux for Power Systems (Little Endian)

Ajout de la prise en charge de Linux for Power Systems (Little Endian) pour les agents de surveillance suivants : Linux OS, WebSphere Application et Db2.

Linux for System x

Ajout de Linux on System x pour prendre en charge le collecteur de données Liberty.

Systèmes d'exploitation Windows 2016

Ajout de la prise en charge pour les systèmes d'exploitation Windows 2016. Pour plus

d'informations, voir le Rapport de compatibilité des produits logiciels (SPCR) pour tous les agents. Dans la section Windows du rapport, recherchez votre système d'exploitation et cliquez sur l'icône de composant pour obtenir la liste des agents pris en charge.

Prise en charge de l'agent de système d'exploitation IBM i

Les données de l'agent de système d'exploitation IBM i peuvent maintenant être affichées dans la console Cloud APM. Cet agent est un agent IBM Tivoli Monitoring V6 et reste un agent V6 pour la version 8.1.4. Vous pouvez utiliser la Passerelle hybride pour extraire les données d'agent et les envoyer au serveur Cloud APM. Ainsi, vous pouvez visualiser les données de surveillance et les événements associés à cet agent dans la console Cloud APM. Pour plus d'informations sur l'agent de système d'exploitation IBM i, voir Hybrid Gateway supported agents (APM Developer Center).

Nouveaux agents disponibles

Monitoring Agent for Amazon EC2

Vous pouvez utiliser l'agent Amazon EC2 pour surveiller la santé, la disponibilité et les performances des ressources de votre instance Amazon Elastic Compute Cloud (EC2). Vous pouvez surveiller les ressources suivantes :

- Utilisation de l'UC
- Utilisation de l'EBS (Elastic Block Store)
- Utilisation du réseau
- Mises à jour de maintenance d'AWS (Amazon Web Services)
- Performances des disques

Cet agent se trouve dans l'Infrastructure Extension Pack.

Monitoring Agent for Cassandra

Vous pouvez utiliser l'agent Cassandra pour surveiller l'état de santé et les performances des ressources du cluster Cassandra, telles que les noeuds, les espaces de clés et les familles de colonne.

Monitoring Agent for Microsoft Office 365

Vous pouvez utiliser l'agent Microsoft Office 365 pour surveiller l'état de santé et les performances des ressources Office 365, telles que les services souscrits d'Office 365, le portail Office 365, les utilisateurs de boîte aux lettres, les sites SharePoint et le stockage OneDrive.

Monitoring Agent for NetApp Storage

Vous pouvez utiliser l'agent NetApp Storage pour surveiller la santé, la disponibilité et les performances des systèmes de stockage NetApp à l'aide de NetApp OnCommand Unified Manager (OCUM). L'agent de surveillance effectue les tâches suivantes :

- Identifie les objets du système de stockage dont les performances sont faibles
- Effectue une reconnaissance et une surveillance à l'aide du serveur OCUM au point focal

Monitoring Agent for OpenStack

Vous pouvez utiliser l'Agent OpenStack pour surveiller la santé et les performances de vos applications OpenStack et afficher des informations, par exemple, sur les noeuds finaux d'API, la connexion au serveur SSH, les processus et les hyperviseurs.

Monitoring Agent for RabbitMQ

Vous pouvez utiliser l'agent RabbitMQ pour surveiller l'état de santé et les performances des ressources du cluster RabbitMQ, telles que les noeuds, les files d'attente et les canaux du cluster.

Monitoring Agent for SAP NetWeaver Java Stack

Vous pouvez utiliser l'Agent SAP NetWeaver Java Stack pour surveiller la santé, la disponibilité et les performances de vos ressources SAP NetWeaver Java Stack Cluster et d'instance. Vous pouvez utiliser l'agent pour surveiller les ressources du cluster, comme les clichés de tas, l'instance de machine virtuelle Java, les détails de transaction, les informations système et les détails de licence. Vous pouvez utiliser l'agent pour surveiller les ressources d'instance, comme l'utilisation de l'UC, l'utilisation de disque, l'utilisation de mémoire, la collecte de bases de données, la récupération de place, les clichés de tas, les applications ayant échoué, le conteneur Web et les informations de session. Vous pouvez également collecter et afficher les données de suivi et de diagnostic des transactions. Ce agent se trouve dans l'Advanced Extension Pack et il est disponible si vous disposez de l'offre Cloud APM, Advanced Private.

Monitoring Agent for Siebel

Vous pouvez utiliser l'agent Siebel pour surveiller l'état de santé et les performances des ressources Siebel, notamment les statistiques Siebel, les sessions utilisateur, les composants, les tâches, le serveur d'applications, le serveur de noms de passerelle Siebel, l'utilisation de la mémoire et de l'UC de processus et la surveillance des événements du journal.

Collecteurs de données nouveaux et améliorés disponibles

Vous pouvez utiliser les collecteurs de données pour surveiller la santé et les performances des applications suivantes sur IBM Cloud et/ou sur site :

collecteur de données J2SE

Vous pouvez utiliser le collecteur de données J2SE pour surveiller la santé et les performances des applications Java et afficher les données de diagnostic, telles que le temps de réponse, la capacité de traitement, le contexte de demande et la trace de méthode des demandes.

collecteur de données Liberty

Le collecteur de données Liberty surveille à la fois le profil Liberty dans l'environnement IBM Cloud et le profil Liberty local sur Linux for System x.

collecteur de données Node.js

Le collecteur de données Node.js surveille à la fois les applications IBM Cloud et sur site. Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

collecteur de données Python

Le collecteur de données Python surveille les applications IBM Cloud. Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

L'Agent Python est supprimé du module d'installation d'agent dans Cloud APM version 8.1.4. Pour pouvez utiliser uniquement le collecteur de données Python pour surveiller vos applications Python.

collecteur de données Ruby

Le collecteur de données Ruby surveille uniquement les applications IBM Cloud. Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

Améliorations au niveau des agents

Monitoring Agent for Citrix Virtual Desktop Infrastructure

- Ajout de la capacité à récupérer les événements du journal des événements Windows pour les machines Virtual Delivery Agent (VDA) et Desktop Delivery Controller (DDC).
- Ajout de la page Sessions VDA, accessible par l'intermédiaire de la page Détails de la machine VDA.
- Ajout du widget des métriques de machine à la page Détails de la machine VDA.
- Amélioration de la configuration DDC (Desktop Delivery Controller) pour permettre à l'agent de traiter la reprise DDC dans un environnement distribution.

Monitoring Agent for Db2

- Ajout de la prise en charge de Linux for Power Systems (Little Endian).
- Ajout de la prise en charge d'Ubuntu ZLinux.
- Un fichier script a été ajouté pour octroyer des privilèges à un utilisateur Db2 de façon à ce qu'il puisse visualiser des données pour l'ensemble des attributs de l'agent Db2 pour une instance surveillée.
- Ajout du support pour Linux for System z.

Monitoring Agent for Hadoop

- Ajout du support pour l'installation et la configuration de l'agent sur les systèmes Windows 2016 et AIX 7.2.
- Ajout du support pour la surveillance des offres Hadoop suivantes : Hortonworks HDP 2.5 et 2.6, Cloudera CDH 5.8 et 5.9, et IBM BigInsights 4.2.
- Ajout du bouton de test de connexion qui permet de vérifier la connexion aux démons Hadoop que vous indiquez lorsque vous configurez l'agent.
- Amélioration du processus de configuration d'agent pour réduire la durée et la complexité de configuration. La configuration a été simplifiée car les tâches de configuration et les prérequis suivants ne sont pas requis :
  - Installation du plug-in sur chaque noeud du cluster Hadoop
  - Configuration et mise à jour du fichier `hadoop-metrics2.properties`
  - Redémarrage des démons Hadoop après la configuration du fichier `hadoop-metrics2.properties`
  - Configuration de tous les DataNodes et NodeManagers dans le cluster
  - Redémarrage de l'agent lors de l'ajout de noeuds supplémentaires au cluster
- Ajout du support pour la surveillance du statut des services Hadoop, tels que ZooKeeper, Sqoop, Hive, HDFS, YARN, Ambari Metrics et Oozie.
- Ajout du support pour la surveillance d'un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO qui utilise uniquement le centre de distribution de clés (KDC) de MIT Kerberos V5.

Monitoring Agent for IBM Integration Bus

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Monitoring Agent for JBoss

Les améliorations suivantes ont été ajoutées à l'agent JBoss :

- Ajout du suivi des transactions et de la surveillance par analyse approfondie dans l'offre Advanced Agents
- Ajout d'une page de tableau de bord pour surveiller les mesures des sources de données
- Ajout de la prise en charge de la surveillance des offres JBoss suivantes : WildFly 8.x/9.x/10.x, JBoss EAP 7.x, JBoss AS 7.x

- Ajout de la prise en charge de l'exécution de l'agent sur le système d'exploitation Windows

Monitoring Agent for Linux KVM

Les améliorations suivantes ont été ajoutées au tableau de bord de l'Agent Linux KVM :

- Le tableau de bord récapitulatif a été mis à jour pour afficher le statut global des hôtes en fonction de l'utilisation de l'UC et de la mémoire de l'application ou de l'environnement de machines virtuelles basées sur le noyau Linux.
- Le tableau de bord Détail d'hôte a été mis à jour pour afficher les détails relatifs à l'hôte sélectionné.
- Le tableau de bord Hôtes, clusters et stockage a été mis à jour pour afficher les détails relatifs aux machines virtuelles surveillées.
- Le widget de groupe Hôtes dans le tableau de bord Hôtes, clusters et stockage a été mis à jour pour afficher les indicateurs clés de performance Mémoire de planification max (Go) et Image instantanée opérationnelle.
- Le tableau de bord Détails de machine virtuelle a été mis à jour pour afficher les détails relatifs à la machine virtuelle sélectionnée sur la page des détails d'hôte.
- Le tableau de bord Détails de stockage a été ajouté pour afficher des détails au sujet des disques et des images instantanées de disque dans le pool de stockage.
- Le widget de groupe Données transmises/reçues sur le réseau (Go) a été ajouté au tableau de bord Détail d'hôte pour afficher des informations historiques sur les données totales (en Go) transmises et reçues sur le réseau.

Monitoring Agent for Linux OS

Ajout du support pour Linux for Power Systems (Little Endian).

Docker version 1.8.0 ou ultérieure est pris en charge. De nouveaux groupes d'attributs et widgets ont été ajoutés afin de permettre à l'agent de système d'exploitation Linux de fournir des fonctionnalités de surveillance Docker.

Monitoring Agent for Microsoft Active Directory

- Ajout de widgets de groupe et de pages pour afficher les détails de Group Policy Object, Netlogon, Local Security Authority et LDAP.
- Ajout des ensembles de données suivants que vous pouvez afficher dans l'onglet **Détails d'attribut** :
  - Ensemble de données de services
  - Réplication
  - File Replication Service (FRS)
  - Unité d'org déplacée ou supprimée
  - Attributs LDAP
  - Gestionnaire de comptes de la sécurité
  - DFS
  - Carnet d'adresses
  - Journal des événements
  - Objets de configuration de mot de passe
- Ajout d'ensembles de données pour ADFS, le proxy ADFS et la file d'attente des unités d'exécution asynchrones.
- Ajout de widgets de groupe et de pages pour afficher les détails d'ADFS et du proxy ADFS.
- Ajout du support pour l'installation et la configuration de l'agent sur les systèmes Windows Server 2016.

Monitoring Agent for Microsoft Exchange Server

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Microsoft Exchange Server :

- Ajout des attributs de temps entrant et sortant dans le jeu de données Accessibilité.
- Ajout de pages et de widgets de groupe pour afficher les détails d'accessibilité.
- Ajout d'un seuil de génération d'événements pour l'accessibilité.
- Support pour l'installation et la configuration de l'agent sur les systèmes Exchange Server 2016 et Windows Server 2016.

Monitoring Agent for Microsoft Internet Information Services

Ajout du support pour l'installation et la configuration sur un système Microsoft Windows Server 2016.

Monitoring Agent for Skype for Business Server

- Ajout du widget de groupe Lync Usage Summary au tableau de bord Lync Server Overview pour afficher le statut d'enregistrement en avant-plan et la qualité des appels médiocres.
- Ajout d'un tableau de bord pour afficher les détails de l'utilisation de Microsoft Lync Server.

Monitoring Agent for Microsoft .NET

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Microsoft .NET :

- Le widget de groupe de statut MS .NET sur la page Composant a été mis à jour pour afficher les temps de réponse des appels de la base de données, le statut des processus .NET dotés d'un nombre d'unités d'exécution élevé et les échecs de compilation Just in Time (JIT).
- Des jeux de données, des pages et des widgets de groupe ont été ajoutés pour afficher les détails de compilation JIT, les détails d'appel de base de données, la collecte des indicateurs GC et des objets réservés pour un processus .NET sélectionné, le taux de conflits d'unité d'exécution et la longueur de la file d'attente d'unités d'exécution.
- Des seuils de génération d'événements ont été ajoutés pour les échecs JIT, les échecs de demande .NET, les commandes lentes, la récupération de place et les unités d'exécution actives dans les processus .NET.

Monitoring Agent for Microsoft SQL Server

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Microsoft SQL Server :

- Le widget de groupe Expensive Queries dans la page Server Performance - Detail a été ajouté pour afficher les 10 premiers plans de requête mis en cache conformément aux statistiques de performance de Microsoft SQL Server.
- Ajout du support pour la surveillance de Microsoft SQL Server 2016.
- Ajout du support pour l'installation et la configuration de l'agent Microsoft SQL Server sur un système Microsoft Windows Server 2016.
- La nouvelle variable d'environnement *COLL_ERRORLOG_RECYCLE_WAIT* a été ajoutée pour définir l'intervalle de temps (en secondes) pendant lequel l'agent attend de collecter les données du groupe d'attributs Détails des événements d'erreur MS SQL.

Monitoring Agent for MongoDB

Les améliorations suivantes ont été ajoutées au tableau de bord de l'Agent MongoDB :

- La page Composant a été mise à jour pour afficher le nombre d'instances MongoDB et leur statut.
- Des pages permettant d'afficher les détails des moteurs de stockage MMAPv1 et WiredTiger ont été ajoutées.
- La page Input Output Information a été ajoutée pour afficher les détails de curseur et les données d'historique des opérations mises en file d'attente, des connexions actives, du flux de données et de l'accès aux données de l'hôte sélectionné.

- Des pages ont été ajoutées pour afficher les détails des verrous version 2.x et version 3.x ou ultérieure.
- La page Détails de la réplication a été ajoutée pour afficher les détails du membre de réplication, d'oplog et des données d'historique du décalage de réplication et de l'espace utilisé par oplog.
- Ajout du support pour la surveillance du cluster MongoDB ou de la configuration de réplication en cas de défaillance du noeud principal.

Monitoring Agent for MySQL

Ajout de jeux de données et d'un paramètre de configuration pour surveiller les ressources MySQL à distance.

Monitoring Agent for Node.js

Les améliorations suivantes ont été ajoutées à l'Agent Node.js pour optimiser les mesures d'application des noeuds (Appmetrics) :

- Nouveaux widgets de tableau de bord et de groupe pour afficher les détails de la récupération de place
- Nouveaux widgets de tableau de bord et de groupe pour afficher les détails des boucles d'événements

Monitoring Agent for Oracle Database

Le tableau de bord de l'agent Oracle Database inclut les nouvelles fonctions suivantes sur la page Détails de l'instance :

- Un tableau contenant des informations sur la contention de verrouillage de l'instance sélectionnée.
- Un tableau contenant des informations sur les services GCS et GES d'Oracle Real Application Clusters.
- Un tableau contenant des informations détaillées sur les groupes de disques de gestion de stockage automatique joints à l'instance sélectionnée.
- Une vue présentant des informations détaillées par espace table, qui s'affiche lorsque vous cliquez sur **Bottom 5 Free**.
- Un tableau contenant des détails historiques sur les processus d'avant-plan et d'arrière-plan joints à l'instance sélectionnée. Vous pouvez cliquer sur l'entité dans le tableau et afficher un tableau détaillé de tous les processus associés à cette instance.
- Un tableau contenant les 5 pires requêtes SQL (par temps d'exécution) associées à l'instance sélectionnée. Vous pouvez cliquer dans le tableau et afficher un tableau détaillé des 50 pires requêtes SQL suivantes associées à cette instance.

Monitoring Agent for PostgreSQL

- Support pour l'installation et la configuration de l'agent sur les systèmes Windows.
- Support pour la surveillance de PostgreSQL V9.6.
- Mise à jour de la page Présentation des statuts de façon à ce que le statut ne soit pas critique lorsque le taux de réussite en mémoire tampon est égal à zéro.

Monitoring Agent for SAP HANA Database

L'attribut Nombre de jours avant expiration de la licence et les seuils HANA_License_Expiry_Crit_SYS et HANA_License_Expiry_Warn_SYS ont été ajoutés pour surveiller le nombre de jours restants avant l'expiration de la licence.

Monitoring Agent for Synthetic Playback

L'Agent Synthetic Playback inclut une nouvelle fonction de filtrage pour les transactions synthétiques. Dans Synthetic Script Manager, configurez des listes noires et des listes blanches pour vos transactions synthétiques qui excluent ou incluent des requêtes vers les

URL et les domaines spécifiés. Utilisez des listes noires et des listes blanches pour filtrer ou inclure les dépendances qui affectent les temps de réponse pour votre application, telles que les métriques de tiers

Vous pouvez maintenant empêcher l'affichage dans Synthetic Script Manager des mots de passe stockés dans des scripts synthétiques.

Monitoring Agent for Tomcat

- Ajout du support pour Linux for System z
- Ajout du support pour l'installation et la configuration de l'Agent Tomcat sur les systèmes Windows et SUSE Linux Enterprise 12.
- Ajout de jeux de données, tableaux de bord et widgets de groupe pour le suivi et les diagnostics approfondis des transactions.

Monitoring Agent for VMware VI

- Mise à jour du widget de groupe Serveur ESX dans le tableau de bord Récapitulatif du serveur pour afficher le statut SSH.
- Ajout de la fonction de découplage de l'agent pour permettre d'afficher et de sélectionner le noeud agent et ses sous-noeuds dans la même vue. Lorsque le composant d'infrastructure virtuelle VMware était sélectionné dans la fenêtre Sélectionner le composant, l'éditeur de composant affichait une structure arborescente du noeud agent avec l'ensemble de ses sous-noeuds.
  - Si l'arborescence était étendue et que l'agent noeud était sélectionné, tous les sous-noeuds étaient sélectionnés automatiquement. Les sous-noeuds à surveiller pouvaient être sélectionnés individuellement.
  - Si un noeud agent était sélectionné lorsque l'arborescence a été réduite, tous les sous-noeuds ont été exclus automatiquement.
  - Lorsque le composant Serveur ESX était sélectionné dans la fenêtre Sélectionner le composant, les serveurs ESX autonomes s'affichaient également dans l'éditeur de composant en plus des sous-noeuds.
  - Avec les sous-noeuds, les serveurs ESX autonomes pouvaient être sélectionnés pour la surveillance.
  - Lorsque l'application était créée, le tableau de bord Interface graphique APM affichait une structure arborescente de l'instance d'agent en tant que parent et ses noeuds en tant qu'enfants.

Monitoring Agent for WebLogic

Le suivi et les diagnostics approfondis des transactions ont été ajoutés à l'agent dans l'offre Advanced Agents.

Monitoring Agent for WebSphere Applications

Ajout de la prise en charge de Linux for Power Systems (Little Endian).

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Ajout du support pour IBM WebSphere Application Server Traditional V9.

Le tableau de bord Analyse de mémoire a été ajouté pour vous aider à diagnostiquer les fuites de mémoire potentielles en vérifiant les informations d'utilisation des segments de mémoire présentées pour chaque cliché de tas. Le mode de diagnostic doit être activé pour que ce tableau de bord contienne des données.

Ajout d'une prise en charge pour utiliser l'ensemble de données Application Health Status afin de créer des seuils d'événement pour la surveillance du statut de l'application. La

collecte de données pour cette utilisation est désactivée par défaut. Vous devez modifier le fichier de propriétés du collecteur de données de façon à l'activer avant de créer des seuils d'événement.

La configuration manuelle du collecteur de données a été simplifiée. Pour WebSphere Applications Server, vous devez seulement ajouter des arguments JVM et des variables pour le serveur d'applications sur la console d'administration WebSphere. Pour Liberty, vous devez uniquement modifier trois fichiers pour le serveur.

Monitoring Agent for WebSphere MQ

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Les données d'historique à long terme de file d'attente et de canal sont prises en charge. Une fois le gestionnaire de files d'attente configuré pour collecter les données statistiques de file d'attente ou de canal, vous pouvez configurer l'agent pour activer la collecte des données d'historique à long terme de file d'attente ou de canal. Bien qu'il n'existe pas de tableau de bord ni de widget prédéfini pour afficher les données d'historique à long terme, vous pouvez utiliser l'onglet **Détails d'attribut** pour demander les données collectées dans vos tables personnalisées.

Agent de surveillance des temps de réponse

- Ajout de la prise en charge de IBM HTTP Server et d'Apache HTTP Server Windows 32 bits (version 8.1.4 Fix Pack 1).
- Ajout d'une prise en charge de la configuration du suivi d'utilisateur pour les applications sur la page Configuration d'agent.
- Ajout d'une prise en charge de la configuration du suivi de session pour les applications sur la page Configuration d'agent.
- Vous pouvez désormais personnaliser les localisations appliquées aux adresses IP ou aux plages d'adresses IP spécifiques dans les tableaux de bord Transaction utilisateur final pour votre environnement spécifique. Utilisez l'onglet **Geolocation** sous **Configuration d'agent** pour personnaliser les valeurs de localisation.

Prise en charge d'IBM OMEGAMON for Application Performance Management

OMEGAMON for APM permet de prendre en charge vos agents IBM OMEGAMON dans votre offre Cloud APM. Les données de l'agent OMEGAMON sont envoyées au serveur Cloud APM par la Passerelle hybride. La Passerelle hybride récupère les données de l'agent OMEGAMON et les événements depuis l'infrastructure IBM Tivoli Monitoring à laquelle les agents OMEGAMON sont connectés. Ainsi, vous pouvez visualiser les données de surveillance et les événements associés à vos agents OMEGAMON dans la console Cloud APM.

La prise en charge d'OMEGAMON for APM n'est disponible que si vous disposez de l'une des offres Cloud APM. Pour installer OMEGAMON for APM, effectuez les étapes de la rubrique «Intégration à OMEGAMON», à la page 905.

Amélioration de la conservation des données

Lorsque vous affichez les descriptions des attributs d'agent ou de collecteur de données dans l'aide ou le guide de référence, chaque jeu de données inclut une instruction sur la fréquence à laquelle les échantillons de données sont envoyés au serveur Cloud APM et sur la durée de stockage de ces échantillons pour les rapports historiques, qui est désormais de huit jours par défaut. Vous pouvez modifier le nombre de jours pendant lesquels les échantillons de données sont sauvegardés jusqu'à 32 jours avant que les échantillons les plus anciens soient supprimés pour laisser la place aux nouveaux.

Amélioration apportée à la fonctionnalité serveur Cloud APM

Lorsque vous vous connectez à un serveur Db2 distant, vous pouvez maintenant spécifier un nom d'utilisateur d'instance Db2 personnalisé. Dans les versions précédentes, l'utilisateur

d'instance Db2 `db2apm` était utilisé. Il n'est pas possible d'utiliser un nom d'utilisateur d'instance Db2 personnalisé si vous effectuez la mise à niveau d'un serveur version 8.1.3.

Amélioration de la visualisation

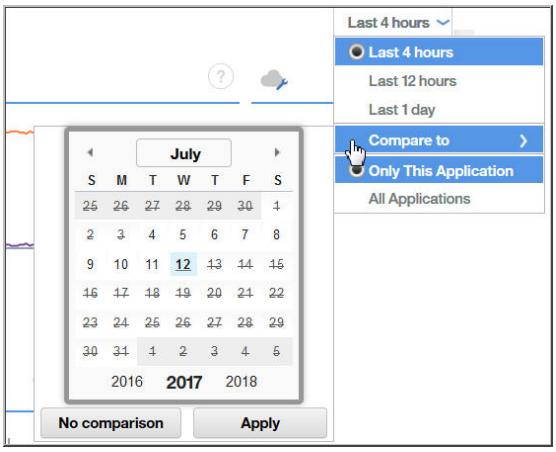
Vues personnalisées

Vous pouvez utiliser la vue Vue universelle d'IBM Cloud Application Business Insights pour créer des pages personnalisées pour les applications que vous surveillez. Dans l'onglet Vues personnalisées, vous pouvez utiliser un modèle existant ou créer des modèles personnalisés pour votre page. Vous avez le choix entre plusieurs options de graphique et de mesure pour créer des widgets permettant de surveiller les données en fonction de vos besoins.

En utilisant la Vue universelle, vous pouvez créer des tableaux de bord pour surveiller les données de plusieurs agents. Vous pouvez exporter les données de pages personnalisées dans un fichier de données brutes. Pour plus d'informations, voir «Vues personnalisées», à la page 1160.

Calendrier pour la comparaison des données d'un jour précédent

Lorsque vous affichez des graphiques à courbes contenant des données d'historique, un calendrier s'ouvre une fois que vous avez choisi une option de sélecteur de temps pour comparer une plage horaire d'un jour précédent. Les jours disponibles pour la comparaison sont barrés. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1138.



Présentation des statuts du Tableau de bord d'Application Performance

La page du Tableau de bord d'Application Performance pour l'application sélectionnée a été rationalisée afin d'améliorer l'affichage. Un comptage des événements de gravité de niveau Avertissement et Critique apparaît sur le titre de l'onglet Evénements et remplace le graphique à barres Récapitulatif de la gravité de l'événement. Dans le cas des applications pour lesquelles des vues de topologie sont activées, la vue Agréger la topologie d'application comporte un bouton bascule permettant de passer au graphique Statut de composant en cours. Pour plus d'informations, voir «présentation des statuts», à la page 1128.

Onglet Détails d'attribut du Tableau de bord d'Application Performance

Pour les utilisateurs malvoyants, la possibilité de créer des tables historiques fournit une alternative aux graphiques à courbes que les technologies d'assistance aux personnes handicapées, telles les logiciels de lecteur d'écran, ne peuvent pas interpréter. Pour cette raison, l'onglet **Détails d'attribut** est disponible pour les instances de transaction de l'Agent de surveillance des temps de réponse et de l'Agent Synthetic Playback pour vous permettre de créer des tables historiques. Pour plus d'informations, voir «Exemple de création d'une table personnalisée avec les commandes du clavier», à la page 1143.

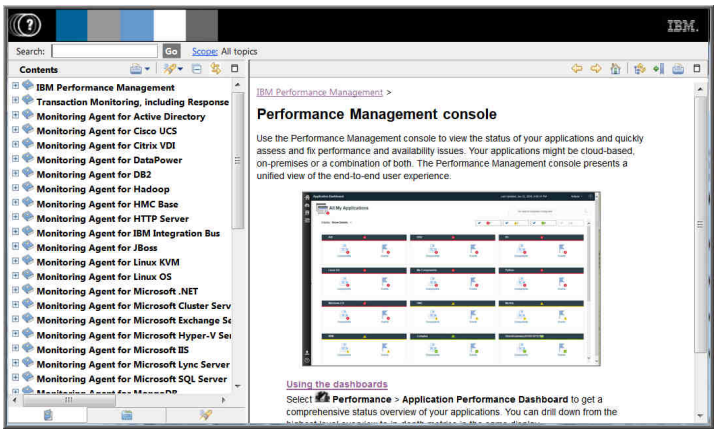
Journal de tableau de bord

Une option de **journal de tableau de bord** a été ajoutée au menu **Actions** pour contrôler la liste des tableaux de bord d'agent mis à jour depuis le dernier redémarrage du serveur. Pour plus d'informations, voir «Toutes mes applications - Tableau de bord d'Application Performance», à la page 1125.

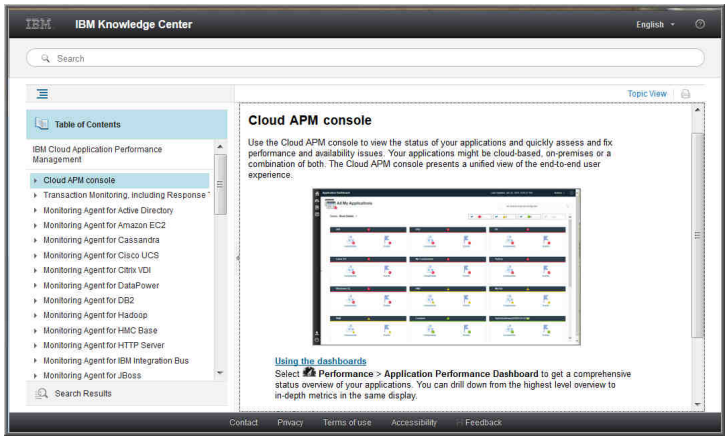
Serveur d'aide IBM Knowledge Center

Dans les précédentes versions, le système d'aide de la console Cloud APM était hébergé sur un serveur d'aide Eclipse. Le système d'aide est maintenant hébergé par IBM Knowledge Center. Vous disposez de l'outil **Masquer la table des matières**, de fonctionnalités de recherche et d'impression, et de liens vers des informations de support et des commentaires en retour.

Avant



Après



Amélioration d'Agent Builder

La prise en charge est améliorée pour la création de tableaux de bord récapitulatifs de Cloud APM pour les agents Agent Builder. Vous devez utiliser des ensembles de données à ligne unique pour fournir des données aux tableaux de bord récapitulatifs. Vous pouvez fournir de tels ensembles de données à partir de fichiers journaux entiers et à partir de tout ensemble de données pouvant être filtré en une ligne unique.

Si vous créez un agent pour surveiller les données d'une base de données JDBC (Java Database Connectivity), vous pouvez modifier les valeurs d'énumération définies pour Erreur, Données manquantes et Aucune valeur, pour éviter tout chevauchement avec les valeurs légitimes de la base de données.

Vous pouvez définir l'autorité d'horodatage des fichiers JAR dans la fenêtre **Préférences** d'Agent Builder. Si le certificat signataire de l'autorité d'horodatage par défaut arrive à expiration, en définissant une nouvelle autorité, vous pouvez continuer de vérifier les fichiers JAR.

Amélioration de l'intégration

Alert Notification
Possibilité de configurer des événements et de les envoyer à Alert Notification. Vous pouvez ensuite configurer des règles afin de déterminer les alertes pour lesquelles vous souhaitez recevoir des notifications. Pour plus d'informations, voir «Intégration à Alert Notification», à la page 908.

Emplacements personnalisables de la fonction d'intégration d'événements pour les événements
Après avoir configuré la transmission d'événements, vous pouvez personnaliser le message d'emplacement de base de la fonction d'intégration d'événements pour les événements envoyés à un récepteur, tel que Netcool/OMNIbus. L'éditeur de seuil comporte une nouvelle zone **Acheminer l'événement de fonction d'intégration d'événements EIF ?** et le bouton **Personnalisation de l'attribut EIF** permettant de personnaliser comment les événements sont mappés vers des événements transmis. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1007.

Plusieurs Passerelles hybrides
Dans les précédentes éditions, vous pouvez installer la Passerelle hybride dans un seul domaine IBM Tivoli Monitoring comportant un Tivoli Enterprise Monitoring Server concentrateur. Vous pouvez maintenant installer une Passerelle hybride dans plusieurs domaines Tivoli Monitoring. La catégorie de Passerelle hybride dans la page Configuration avancée de la console Cloud APM a été déplacée vers sa propre page Gestionnaire de passerelle hybride. Vous pouvez créer et modifier les profils Passerelle hybride pour les systèmes gérés de surveillance à partir de plusieurs domaines Tivoli Monitoring, un profil pour chaque domaine. Pour plus d'informations, voir «Passerelle hybride», à la page 875.

Evolutivité améliorée
Augmentation du nombre maximal de systèmes gérés que vous pouvez surveiller à partir d'un Cloud APM, Private de 4 000 à 10 000 systèmes gérés.

API Vous pouvez utiliser les API pour créer des scripts afin d'automatiser l'intégration de votre environnement Performance Management. Pour plus d'informations, voir «Exploration des API», à la page 1115.

Versions précédentes

Pour plus d'informations sur les nouvelles fonctions et options des éditions précédentes, reportez-vous aux rubriques *Nouveautés* suivantes :

- Nouveautés : version 8.1.3
- Nouveautés : version 8.1.2
- Nouveautés : version 8.1.1

Considérations à prendre en compte pour la mise en conformité avec le règlement RGPD

Informations relatives aux fonctions que vous pouvez configurer et aux aspects du produit que vous devez prendre en compte pour aider votre organisation à se mettre en conformité avec le règlement RGPD.

Considérations relatives au règlement RGPD pour les offres suivantes :

- IBM Cloud Application Performance Management Private
- IBM Tivoli Monitoring
- IBM Tivoli Composite Application Manager
- IBM SmartCloud Monitoring

- Application Insight

Pour les ID produit :

5725-G70

5725-I45

5724-U17

5724-S79

5724-C04

5725-C20

5724-L92

5725-J97

5725-U05

5725-V20

5725-M99

- **Remarque :**
  L'objectif de ce document est de vous aider à préparer la mise en conformité avec le règlement général sur la protection des données (RGPD). Le document contient des informations sur les fonctions que vous pouvez configurer dans les offres et sur les aspects du produit que vous devez prendre en compte pour aider votre organisation à se mettre en conformité avec le règlement RGPD. Ces informations ne constituent pas une liste exhaustive, en raison des nombreuses façons dont les clients peuvent choisir et configurer les fonctions et du large éventail des modes d'utilisation du produit seul et avec des applications et systèmes tiers.**Il appartient à chaque entreprise de se conformer aux lois et réglementations, notamment au règlement général sur la protection des données de l'Union européenne. Il relève de la seule responsabilité du client de consulter les services juridiques compétents aussi bien pour identifier et interpréter les lois et règlements susceptibles d'affecter son activité, que pour toute action à entreprendre pour se mettre en conformité avec ces lois et réglementations.**

  Les produits, services et autres fonctionnalités décrits ici ne sont pas adaptés à toutes les situations client et ne pourront être proposés que sous réserve de disponibilité. IBM ne donne aucun avis juridique, comptable ou d'audit et ne garantit pas que ses services ou produits assurent la conformité des clients aux lois applicables.

Table des matières

1. «RGPD», à la page 23

2. «Configuration de produit pour la mise en conformité avec le règlement RGPD», à la page 23

3. «Cycle de vie des données», à la page 24

3. «Collecte des données», à la page 24

5. «Stockage des données», à la page 25

6. «Accès aux données», à la page 26

7. «Traitement des données», à la page 26

8. «Suppression des données», à la page 27

9. «Surveillance des données », à la page 27

10. «Réponse aux droits des Personnes concernées», à la page 28

RGPD

Le règlement général sur la protection des données (RGPD) a été adopté par l'Union européenne (UE) et s'applique depuis le 25 mai 2018.

Pourquoi le règlement RGPD est-il important ?

Le règlement RGPD établit une infrastructure réglementaire plus forte sur la protection des données pour le traitement des données personnelles des personnes physiques.

Le RGPD apporte :

- Des droits nouveaux et renforcés aux personnes physiques
- Une définition élargie des données personnelles
- De nouvelles obligations pour les organisations qui traitent les données personnelles
- Des pénalités financières lourdes en cas de non-respect
- Une notification obligatoire des atteintes à la protection des données
- **En savoir plus sur le règlement RGPD**
  - [Portail d'informations sur le règlement RGPD de l'Union européenne] (https://www.eugdpr.org/)
  - [Site Web ibm.com/GDPR] (https://www.ibm.com/data-responsibility/gdpr/)

Configuration de produit pour la mise en conformité avec le règlement RGPD

Les sections ci-dessous incluent des remarques pour configurer le produit et vous aider à mettre votre organisation en conformité avec le règlement RGPD.

- **Configuration respectant les exigences en matière de manipulation des données**

  Le règlement RGPD (Règlement général sur la protection des données) exige que les données personnelles soient strictement contrôlées et que l'intégrité des données soit assurée. Pour cela, les données doivent être protégées contre toute perte due à un incident système et à un accès non autorisé ou par le biais d'un vol d'équipement informatique ou de support de stockage.
- **Comment configurer notre offre pour pouvoir l'utiliser dans un environnement RGPD ?**

  IBM® Cloud Application Performance Management Private (Cloud APM Private) est une solution complète qui vous aide à gérer les performances et la disponibilité des applications déployées sur site (privées) dans un cloud public ou comme combinaison hybride. Cette solution fournit une visibilité sur les applications, et permet de les contrôler et de les automatiser, garantissant ainsi des performances et une utilisation des ressources optimales.

  IBM Tivoli Monitoring (ITM) surveille et gère les applications système et réseau sur un grand nombre de systèmes d'exploitation, suit la disponibilité et les performances du système d'entreprise et fournit des rapports pour suivre des tendances et résoudre des problèmes métier.

  L'offre IBM Tivoli Composite Application Manager (ITCAM) for Applications est un module de produits qui surveillent et gèrent des systèmes, des serveurs d'applications et des serveurs de bases de données, suivent la disponibilité et les performances et fournissent des rapports dans une interface graphique utilisateur basée sur un navigateur pour suivre les tendances et résoudre les problèmes.

Les données sont envoyées à l'interface utilisateur APM et ITM à partir du système d'exploitation, des applications, des agents de langage de codage ou des collecteurs de données. Ces données sont ensuite stockées dans une base de données IBM Db2. L'utilisateur crée des événements à partir de ces données pour les conditions anormales à surveiller.

Pour les bases de données Oracle ou SQL, reportez-vous à la documentation du fournisseur approprié.

Cycle de vie des données

Le règlement RGPD exige que les données à caractère personnel soient :

- traitées de manière licite, loyale et transparente au regard des personnes concernées ;
- collectées pour des finalités déterminées, explicites et légitimes ;
- adéquates, pertinentes et limitées à ce qui est nécessaire ;
- exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées sans tarder ;
- ne soient conservées sous une forme permettant l'identification des personnes concernées que pendant la durée nécessaire.
- **Quel est le processus de bout en bout par lequel passent les données personnelles lors de l'utilisation de notre offre ?**
- **Données à caractère personnel utilisées pour les contacts en ligne avec IBM**

Les clients de *l'offre* peuvent soumettre des commentaires, des remarques et des demandes en ligne pour contacter IBM sur différentes aspects de l'offre de plusieurs manières, notamment :

- La zone de commentaires publics sur les pages de la communauté des offres dans IBM developerWorks
- Zone de commentaires publics dans les pages de la documentation de l'offre dans IBM Knowledge Center
- Commentaires publics dans l'espace de l'offre de dWAnswers
- Formulaires de commentaires dans la communauté de l'offre

En règle générale, seuls le nom et l'adresse électronique du client sont utilisés pour permettre des réponses personnelles pour l'objet du contact et l'utilisation des données à caractère personnel se conforme à [la Déclaration IBM de confidentialité sur Internet] (https://www.ibm.com/privacy/us/en/).

- Quels types de données ?

  Les offres Application Performance Management/Tivoli Monitoring ne ciblent et ne collectent pas directement les données personnelles. Le type de données collectées par les produits correspond principalement à des mesures de gestion des performances qui évaluent les performances d'un système d'exploitation sous-jacent, d'application comme des serveurs Web et des bases de données ou des langages de codage, comme .Net, python ou ruby.

  Les offres Application Performance Management/Tivoli Monitoring assurent l'authentification et le traitement des utilisateurs système.

  Les offres Application Performance Management/Tivoli Monitoring traitent les types de données personnelles présentées ici :

  – Données d'authentification (telles que le nom d'utilisateur et le mot de passe).
  – Informations personnelles techniquement identifiables (ID d'unité, identificateurs basés sur l'utilisation ou adresse IP liée à une personne) utilisées pour identifier les systèmes ou les applications surveillés lors d'un fonctionnement normal de ce produit.

Collecte des données

Cette liste n'est pas une liste exhaustive des types de données collectées par les offres. Elle est fournie à titre d'exemple pour alimenter votre réflexion. Pour toute question sur les types de données, contactez IBM.

Les données sont collectées par des agents qui se connectent à des systèmes d'exploitation et à des applications d'IBM et de fournisseurs tiers pour aider l'utilisateur final à vérifier le niveau de performances de ces systèmes ou de ces applications.

Aucun de ces éléments ne cible les données à caractère personnel ; toutefois, les éléments suivants peuvent figurer dans le produit dans le cadre de la procédure de surveillance :

- Les données d'authentification (comme les noms d'utilisateur et les mots de passe)
- Les informations personnelles techniquement identifiables (ID d'unité, identificateurs basés sur l'utilisation ou adresse IP liée à une personne, etc.)

Stockage des données

- **Comment le client peut-il contrôler le stockage des données personnelles ?**

  Les offres Application Performance Management/Tivoli Monitoring utilisent une instance Db2 pour stocker des données de gestion des performances, qui n'incluent pas de données personnelles par défaut.
- Stockage des données de compte

  Les noms d'utilisateur et les mots de passe peuvent être gérés de plusieurs manières dans les offres Application Performance Management/Tivoli Monitoring. Les utilisateurs peuvent être authentifiés auprès du serveur TEPS ou d'un référentiel externe, comme un annuaire LDAP ou un référentiel basé sur les fichiers (géré par Websphere Application Server). Afin de faciliter l'administration des utilisateurs, il est recommandé de centraliser la gestion des utilisateurs à l'aide du service d'annuaire central des organisations.

  Pour plus d'informations sur la configuration des offres Application Performance Management/Tivoli Monitoring pour utiliser un service d'annuaire externe comme source d'authentification, voir :

  https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_ldap.htm

  https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/msad_ldap_enabletems.htm
- Stockage des données client

  Les principales données traitées par les offres Application Performance Management/Tivoli Monitoring sont liées à des données de mesure de performances qui, en fonction de l'environnement de déploiement utilisé, peuvent être des données qui vous appartiennent ou qui proviennent de l'environnement du client final. Les offres Application Performance Management/Tivoli Monitoring incluent des contrôles d'accès basés sur des rôles et des groupes, ainsi que des filtres de restriction pour contrôler l'accès aux données d'événement en cours.

  Pour plus d'informations, voir :

  https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_workingwithrolesusersandpermissions.htm

  https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/authpolicy_intro.htm
- Stockage dans des copies de sauvegarde

  Vous pouvez utiliser Db2 pour configurer des sauvegardes. Pour plus d'informations, voir :

  https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_backup_online_dbs.htm

  https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/install/backup_ps_db.htm
- Stockage dans des archives.

  Pour plus d'informations, voir : https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/historyconvert_zosmanarchive.htm
- Chiffrement des données

Pour plus d'informations, voir : https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/security_encryptintro.htm

Accès aux données

Utilisez la fonction de contrôle d'accès basé sur les rôles dans IBM Cloud Application Performance Management pour accorder aux utilisateurs les droits d'accès dont ils ont besoin pour leur rôle.

La sécurité de Cloud APM Private est basée sur des rôles. Un rôle est un groupe de droits d'accès qui contrôlent les actions que vous pouvez effectuer dans Cloud APM Private. Vous pouvez créer des rôles personnalisés dans Cloud APM Private. Vous pouvez affecter des droits à des rôles personnalisés ou davantage de droits aux rôles par défaut existants.

Vous pouvez affecter des utilisateurs et des groupes d'utilisateurs à des rôles par défaut existants ou à des rôles personnalisés. Vous pouvez affecter des utilisateurs et des groupes d'utilisateurs à plusieurs rôles. Les droits sont cumulatifs, un utilisateur ou un groupe est affecté à tous les droits de tous les rôles auxquels il est affecté. Cloud APM Private utilise le registre de base des profils Liberty de WebSphere Application Server comme méthode par défaut pour l'authentification des utilisateurs. Vous pouvez également utiliser un registre LDAP à cet effet.

Pour plus d'informations, voir :

- Gestion des accès utilisateur

  https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_security.htm
- Rôles et droits d'accès

  https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_workingwithroles.htm
- Contrôle d'accès basé sur les rôles

  https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/authpolicy_intro.htm

  https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_workingwithrolesusersandpermissions.htm
- Authentification utilisateur :

  https://www.ibm.com/support/knowledgecenter/SS3JRN_7.2.1/com.ibm.itm.doc_6.3fp2/adminuse/userauthenticate_intro.htm

  https://www.ibm.com/support/knowledgecenter/SS3JRN_7.2.1/com.ibm.itm.doc_6.3fp2/adminuse/user_administerintro_tep.htm

  https://www.ibm.com/support/knowledgecenter/SS3JRN_7.2.1/com.ibm.itm.doc_6.3fp2/adminuse/user_administerintro_tep.htm

Traitement des données

- **Comment le client peut-il contrôler le traitement des données personnelles ?**
- Chiffrement des données en mouvement

  Les offres Application Performance Management/Tivoli Monitoring peuvent être configurées pour utiliser des communications SSL pour les données transmises par les composants.
- Chiffrement des communications des agents avec le serveur

  Les agents ITM exécutés en mode autonome ou via une gestion centralisée incluent de nouvelles options pour les déploiements hautement sécurisés des agents de surveillance. Après avoir exécuté quelques opérations de configuration rapides dans l'environnement à l'issue de l'installation, les clients peuvent effectuer des déploiements hautement sécurisés des agents de surveillance dans des environnements fortement contraints comme DMZ.

Le modèle de déploiement des agents autonomes est comparable au modèle de déploiement des agents ITM standard gérés de manière centralisée dans lequel les agents communiquent avec leur infrastructure via des connexions sécurisées et utilisent des fichiers de configuration locaux que les administrateurs peuvent gérer.

Dans un environnement sécurisé, les agents sont invisibles pour le trafic réseau extérieur ; ils réduisent leurs voies de communication et verrouillent l'accès aux fichiers d'agent sur le système de fichiers. Une configuration hautement sécurisée garantit également un chiffrement authentifié renforcé sur toutes les voies de communication.

Ce livre blanc répertorie les étapes nécessaires pour verrouiller les connexions réseau ouvertes par défaut et vérifie que l'installation est sécurisée de l'intérieur.

Pour plus d'informations, voir https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli+Monitoring/page/Creating+a+Highly+Secure+IBM+Tivol+Monitoring+Agent+Configuration

Pour plus d'informations, voir https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/onprem_config_https.htm

https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/install/unixconfig_ma.htm

- Configuration de la communication TLS/SSL entre le serveur de portail et le serveur LDAP

  Pour plus d'informations, voir https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/userauthenticate_tepsldap_ssl.htm

Suppression des données

- **Comment le client peut-il contrôler la suppression des données personnelles ?**
  - Suppression des données client

    La suppression des utilisateurs de l'une des offres Application Performance Management/Tivoli Monitoring, du service de référentiel basé sur des fichiers ou du service d'annuaire externe empêche l'utilisateur de se connecter au produit. Cette l'opération ne supprime pas les données de l'utilisateur, comme son nom, des événements actifs ou historiques car le système a toujours besoin de gérer ces données d'un point de vue opérationnel ou d'audit. Cependant, dans le cadre de votre déploiement, il est recommandé d'examiner la période pendant laquelle les données sont archivées, les sauvegardes stockées et les journaux conservés afin de déterminer si elle est adaptée à vos besoins opérationnels.

    Pour supprimer des données de la base de données Db2, reportez-vous à Db2 Knowledge Center :

    https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.welcome.doc/doc/welcome.html

    Pour les autres bases de données, reportez-vous à la documentation du fournisseur de la base de données.
- Suppression des données de compte

  La suppression des utilisateurs de l'un des modules Application Performance Management/Tivoli Monitoring, du service de référentiel basé sur des fichiers ou du service d'annuaire externe empêche l'utilisateur de se connecter au produit. Cette opération ne supprime pas les données de l'utilisateur, comme son nom, des événements actifs ou historiques car le système a toujours besoin de gérer ces données d'un point de vue opérationnel ou d'audit. Cependant, dans le cadre de votre déploiement, il est recommandé d'examiner la période pendant laquelle les données sont archivées, les sauvegardes stockées et les journaux conservés afin de déterminer si elle est adaptée à vos besoins opérationnels.

  Pour supprimer un utilisateur et son accès du produit, voir https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_workingwithrolesusersandpermissions.htm

Surveillance des données

- **Comment le client peut-il contrôler le traitement des données personnelles ?**

- Les offres Application Performance Management/Tivoli Monitoring permettent de surveiller les serveurs, les systèmes d'exploitation, les applications et le code dans une entreprise. Dans le produit, les données personnelles sont limitées aux éléments suivants :
  - Les informations personnelles de base, comme les noms d'utilisateur pour l'authentification
  - Les informations personnelles techniques (par exemple adresses IP/noms d'hôte des systèmes permettant à l'utilisateur d'accéder à la solution et éventuellement capturés dans les journaux de débogage/trace).

  La base de données du produit peut être configurée pour auditer l'accès à des objets spécifiques ou les actions effectuées par des groupes d'utilisateurs spécifiques dans des journaux d'audit, comme indiqué précédemment.

  Les fichiers journaux ne sont pas chiffrés. Si vous devez les archiver pour des raisons opérationnelles/d'audit, envisagez de les chiffrer.

Configuration de la journalisation d'audit

Pour plus d'informations, voir :

- APM : https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_configuringauditlogging.htmhttps://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_auditlogger.htm
- ITM : https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/adminuse/agentadmin_audit_intro.htm
- Journalisation d'audit de Db2 : https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/c0005483.html

Réponse aux droits des Personnes concernées

- **Dans quelle mesure l'offre facilite-t-elle le respect des droits des personnes ?**

  Les données personnelles stockées et traitées par le produit appartiennent aux catégories suivantes :
- Données personnelles de base, comme les noms d'utilisateur et les mots de passe utilisés pour l'authentification et le nom/ID indiquant le propriétaire de l'événement
- Informations personnelles d'identification techniques (comme les adresses IP ou les noms d'hôtes auxquels l'activité de l'utilisateur peut être liée)

  Ces données font partie intégrante du fonctionnement d'un flux de travaux de gestion des performances efficace. Le retrait des données, la modification des données historiques et le partage de ces données sont probablement des opérations contraires aux politiques de votre entreprise.

Toutefois, prenez bien en compte les points suivants :

- Les données ne sont conservées que pendant une période raisonnable en fonction des besoins d'exploitation, de conformité et d'audit applicables.
- Les données sont sécurisées de manière appropriée lorsqu'elles sont archivées.
- Les termes du contrat sont compatibles avec le règlement RGPD pour les éléments suivants :
  - Lorsque le produit est utilisé pour gérer vos entreprises, votre propre environnement informatique/réseau ou vos applications.
  - Lorsque les utilisateurs de la solution sont des employés ou du personnel liés par un engagement contractuel.
  - Lorsque les schémas d'événement sont personnalisés pour compléter les valeurs par défaut avec des informations supplémentaires provenant d'autres sources de données disponibles dans votre environnement, par exemple des données personnelles.

Chapitre 2. Documentation au format PDF

Des documents PDF compilent les rubriques de cette collection IBM Knowledge Center sous la forme de guides d'utilisation. Des références sont également disponibles pour chaque agent.

IBM Knowledge Center

Outre ce Guide d'utilisation, vous pouvez télécharger le document IBM Agent Builder - Guide d'utilisation.

Référence d'agent

Pour télécharger la référence pour un agent, voir Agent metrics/Reference PDFs sur Application Performance Management Developer Center. Les références fournissent des informations sur les tableaux de bord, les seuils de génération d'événement et les ensembles de données. Les ensembles de données contiennent des attributs, qui sont les mesures signalées par l'agent et qui constituent les indicateurs clés de performance (KPI). La version de l'agent apparaît sur la page de titre du fichier PDF.

Aide en ligne

En outre, vous pouvez accéder à l'aide en ligne lorsque vous êtes connecté à la console Cloud APM en cliquant sur **Aide** > **Contenu de l'aide** dans la barre de navigation. Vous pouvez également explorer la Démonstration dynamique de Cloud APM et accéder à l'aide de la console Cloud APM ici.

© Copyright IBM Corp. 2015, 2018

Chapitre 3. Présentation du produit

IBM Cloud Application Performance Management (Cloud APM) est une solution complète qui vous aide à gérer les performances et la disponibilité des applications déployées sur site(privées), dans un cloud public ou comme combinaison hybride. Cette solution fournit une visibilité sur les applications, et permet de les contrôler et de les automatiser, garantissant ainsi des performances et une utilisation des ressources optimales.

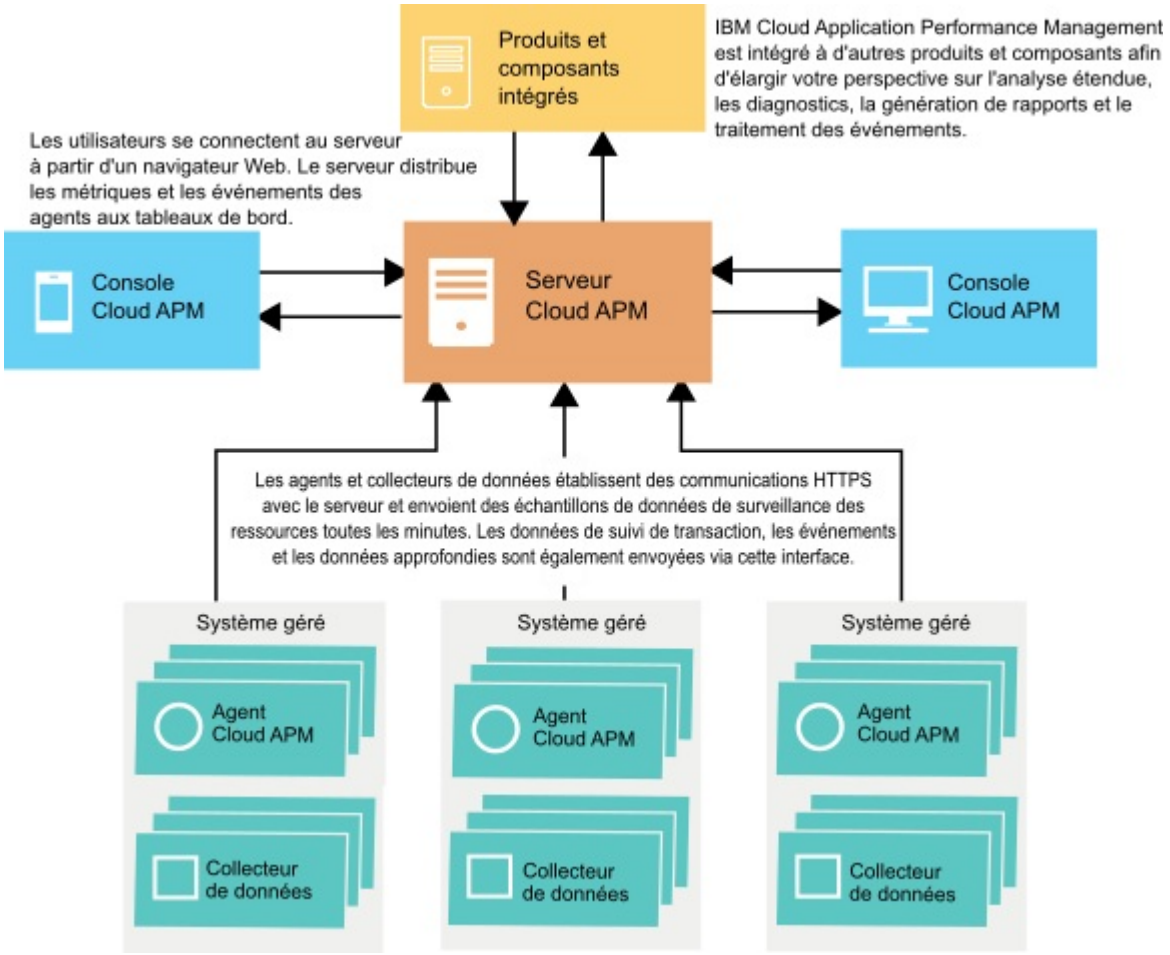
Cette solution permet de gérer le centre de données, l'infrastructure de cloud et les charges avec une intelligence cognitive. Vous pouvez réduire et empêcher les indisponibilités et les ralentissements dans un environnement d'applications hybrides car Cloud APM vous aide à passer de l'identification des problèmes de performances à l'isolement de l'endroit où le problème se produit et au diagnostic des problèmes avant qu'ils n'affectent votre activité.

Utilisez les fonctionnalités principales, qui varient selon l'offre, pour utiliser les données recueillies par les agents et les collecteurs de données Cloud APM. Plus de fonctionnalités sont disponibles grâce à l'intégration aux autres produits et composants.

© Copyright IBM Corp. 2015, 2018

Présentation de l'architecture

IBM Cloud Application Performance Management utilise des *agents* et les *collecteurs de données* pour collecter des données sur des hôtes surveillés. Les agents et les collecteurs de données transmettent les données au serveur Cloud APM, qui les assemble dans la console Cloud APM.



Collecte de données

Les agents et les collecteurs de données surveillent des systèmes, des sous-systèmes ou des applications et collectent des données. Un agent ou un collecteur de données interagit avec une seule ressource (par exemple, un système ou une application) et, dans la plupart des cas, se trouve sur l'ordinateur ou la machine virtuelle où s'exécute le système ou l'application. Par exemple, l'Agent Linux OS collecte des indicateurs de performance pour le système d'exploitation sur l'hôte Linux et l'Agent WebSphere Applications surveille les indicateurs de performance des serveurs d'applications WebSphere. Il existe également des agents qui suivent les transactions entre les différentes ressources.

Vous pouvez configurer des seuils pour les indicateurs clés de performance. Lorsqu'un indicateur passe au-dessus ou en-dessous du seuil, l'agent ou le collecteur de données génère une alerte que le serveur traite. Vous pouvez également configurer le transfert des événements vers une cible telle que la Netcool/OMNIbus Probe for Tivoli EIF ou un serveur SMTP et utiliser la fonction Alert Notification pour configurer les notifications par courrier électronique pour les événements.

Les agents et les collecteurs de données sont préconfigurés pour communiquer avec le serveur Cloud APM.

Communication entre le serveur et les agents ou les collecteurs de données

Les agents et les collecteurs de données de chaque hôte surveillé établissent des communications HTTP avec le serveur Cloud APM. L'agent ou le collecteur de données constitue le côté client de la connexion.

Si vous avez configuré les communications HTTPS et que vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer les agents pour l'envoi du trafic à un proxy direct. Pour plus d'informations, voir «Connectivité réseau», à la page 201.

serveur Cloud APM

Le serveur Cloud APM reçoit et traite les informations de surveillance provenant de tous les agents et collecteurs de données de votre infrastructure. Le serveur fournit également la console Cloud APM. Vous pouvez utiliser un navigateur Web pour accéder à la console et afficher les informations recueillies.

Lorsque vous installez le serveur Cloud APM, le programme d'installation déploie également une base de données Db2 et une base de données MongoDB. Vous pouvez utiliser un serveur Db2 ou un serveur MongoDB existant à condition qu'ils ne soient pas installés sur le même serveur que le serveur Cloud APM et que leurs versions soient compatibles pour 8.1.4.0.

Le programme d'installation préconfigure également une copie des agents et des collecteurs de données pour communiquer avec ce serveur. Vous pouvez utiliser le serveur pour générer ultérieurement une copie préconfigurée des agents et des collecteurs de données.

Données stockées par le serveur

Les agents et les collecteurs de données envoient les données au serveur Cloud APM à des intervalles compris entre 1 minute et 8 minutes, en fonction de type des données. Le serveur stocke toutes les valeurs envoyées par les agents et les collecteurs de données pendant 8 jours par défaut. Des données de transaction résumées sont stockées pendant de plus longues périodes.

Les données de surveillance sauvegardées sont appelées *données d'historique*. Le serveur se sert des données d'historique pour afficher des tableaux et des graphiques qui vous permettent d'analyser les tendances de votre environnement. Vous pouvez modifier le nombre de jours pendant lesquels les échantillons de données sont conservés. Par défaut, ce nombre est de 8 jours ; les valeurs recommandées (comprises entre 2 et 32 jours) ont été établies par les développeurs de l'agent et du collecteur de données.

Des rapports d'historique sont également disponibles pour certains agents. Pour plus d'informations, voir «Rapports», à la page 1172.

Evolutivité

Vous pouvez surveiller jusqu'à 10 000 systèmes gérés à partir de Cloud APM, Private. Un système géré est un système d'exploitation, un sous-système ou une application unique de votre entreprise surveillé par un agent.

Le nombre réel de systèmes gérés pouvant être pris en charge par votre environnement dépend du nombre et du type des agents dans votre environnement et de la capacité de votre serveur Cloud APM. Un élément clé est le nombre de lignes de données d'agent écrites dans la base de données par minute. Utilisez la feuille de calcul disponible dans Load projections (APM Developer Center) pour estimer le nombre de lignes d'agent écrites par minute. Comparez les résultats avec la plage de valeurs pour les différentes tailles d'environnement dans le tableau 1 ou le tableau 2 dans «Configuration matérielle requise pour le serveur Cloud APM», à la page 92. Pour l'offre Cloud APM, Advanced Private, un élément supplémentaire à prendre en compte est le nombre de transactions utilisateur surveillées par seconde.

Intégration

IBM Cloud Application Performance Management est intégré avec d'autres produits et composants si ceux-ci sont configurés pour la communication avec le serveur Cloud APM.

Les produits qui peuvent être intégrés incluent Netcool/OMNIbus, Tivoli Monitoring, OMEGAMON for APM, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, IBM Alert Notification, Tivoli Common Reporting et IBM Cloud.

Agent Builder est un composant qui peut être utilisé pour créer des agents personnalisés.

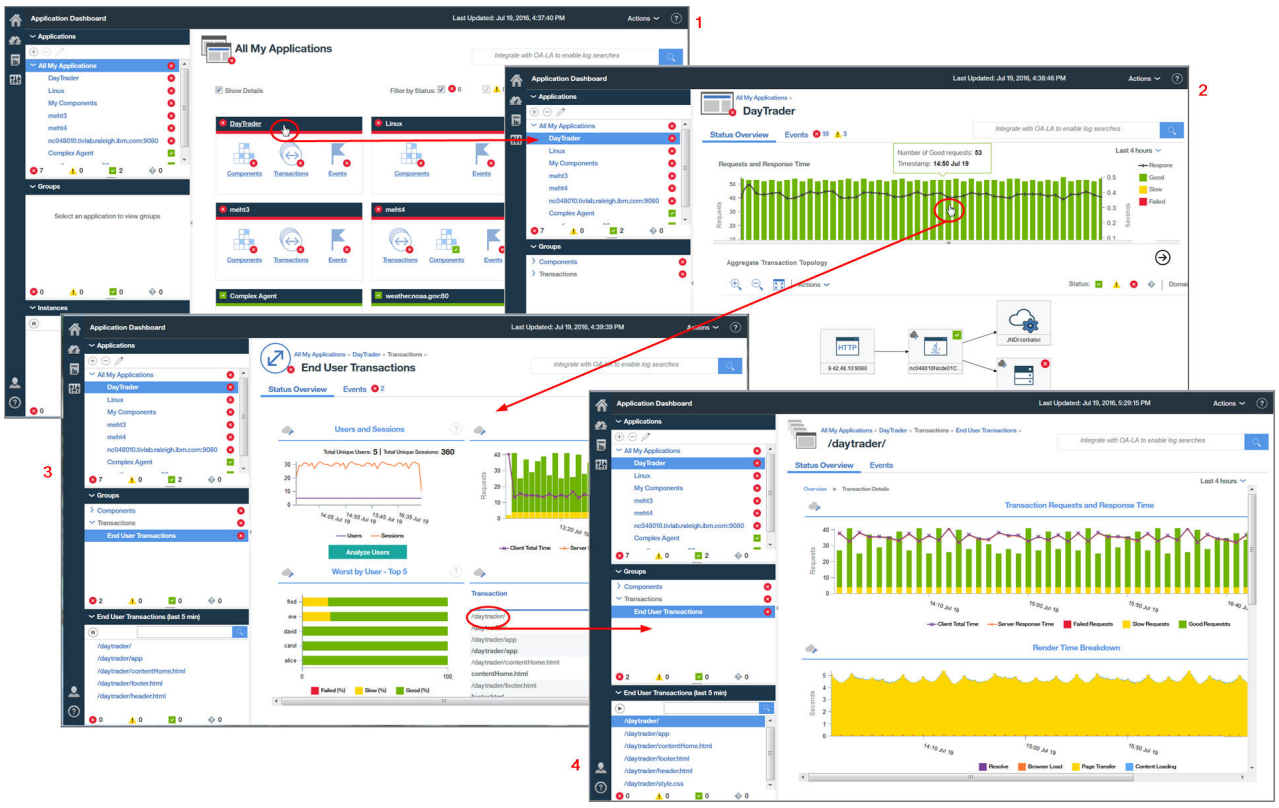
Interface utilisateur

La console Cloud APM est l'interface utilisateur de Cloud APM. Cette interface utilisateur unifiée fournit une vue unique au sein d'applications hybrides. Vous pouvez utiliser la console pour afficher le statut des applications et évaluer et résoudre rapidement les problèmes de performances et de disponibilité.

Les tableaux de bord de la console facilitent l'identification des problèmes pour vous permettre d'isoler les goulots d'étranglement qui affectent les performances des applications. A l'aide d'une simple navigation dans les tableaux de bord, vous pouvez passer d'une vue présentant le statut de l'application à des informations détaillées au niveau du code. Vous pouvez visualiser les problèmes du code source au moment exact de leur apparition. Vous pouvez rechercher et diagnostiquer des problèmes à l'aide des données d'analyse de recherche intégrées.

Le navigateur du Tableau de bord d'Application Performance dans la console est hiérarchique, ce qui vous permet d'avoir une vue globale du statut de vos applications, de la santé de leurs composants et de la qualité de l'expérience de leurs utilisateurs. Pour plus de détails sur la ressource surveillée, vous pouvez cliquer sur un élément de navigateur ou sur un lien dans les vues du tableau de bord. Imaginez, par exemple, que votre application présente un temps de réponse long. Le problème est signalé dans le tableau de bord. A partir du tableau de bord, vous pouvez remonter jusqu'à la source du problème en cliquant sur des liens pour en identifier la cause (par exemple, une utilisation élevée de l'unité centrale sur le système en raison d'un processus hors de contrôle).

Pour plus d'informations sur l'utilisation des tableaux de bord dans la console Cloud APM, voir Chapitre 14, «Utilisation des tableaux de bord», à la page 1125.



Offres et modules complémentaires

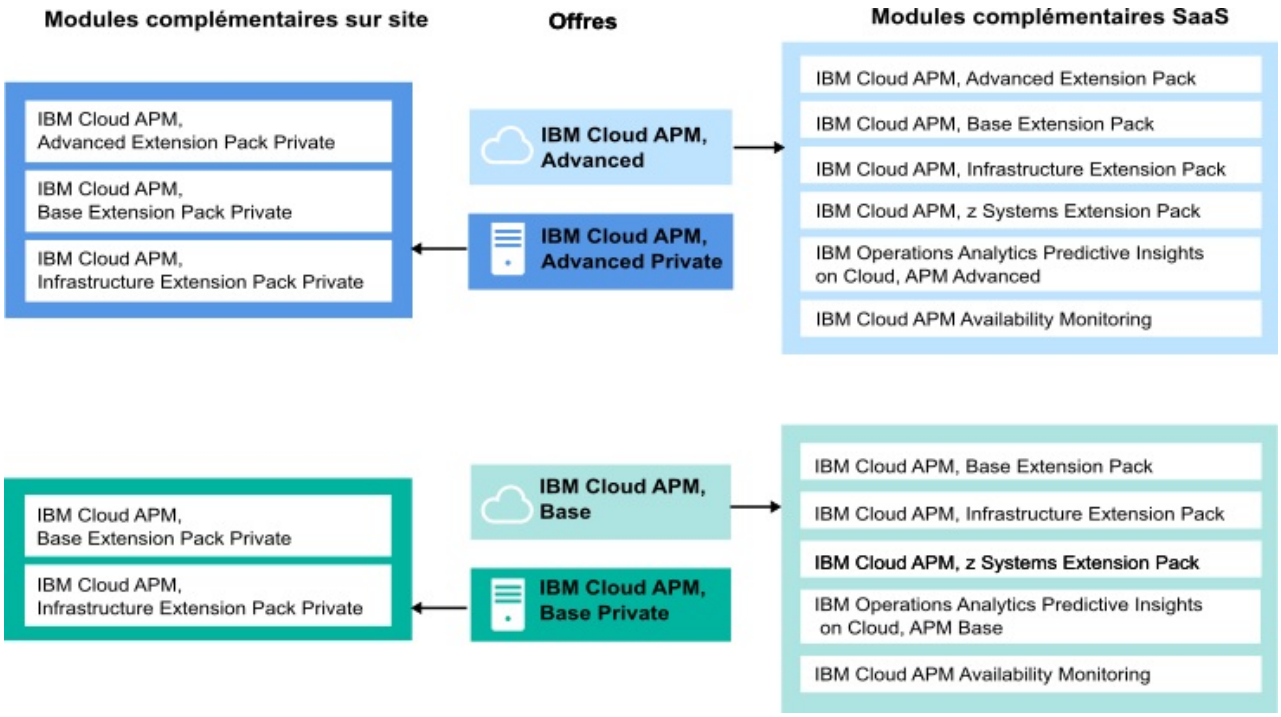
Il existe deux offres IBM Cloud Application Performance Management, Private, Base et Advanced, et plusieurs modules complémentaires. Les offres et modules complémentaires contiennent des agents et des collecteurs de données. Des modules complémentaires spécifiques peuvent être utilisés avec chaque offre.

Les offres IBM Cloud Application Performance Management, Private (anciennement appelées IBM Performance Management) et certaines extensions de produit ont été renommées et consolidées dans la version 8.1.4. Pour plus d'informations, voir «Nouvelle stratégie de marque et simplification du produit», à la page 10.

Pour savoir quels agents sont inclus dans une offre ou un module complémentaire et découvrir les fonctionnalités d'agent et de collecteur de données, voir «Fonctions», à la page 40.

Pour chaque offre, des modules complémentaires sont disponibles dans IBM Passport Advantage. IBM Cloud Application Performance Management, Advanced Private est l'offre la plus complète, elle inclut tous les agents, tous les collecteurs de données et toutes les pages de tableau de bord. IBM Cloud Application Performance Management, Base Private est un sous-ensemble d'Cloud APM, Advanced. Vous pouvez remplacer Cloud APM, Base par Cloud APM, Advanced à tout moment. L'offre finale installée après ce remplacement est Cloud APM, Advanced. Le diagramme indique quels modules complémentaires sont disponibles pour chaque offre.

Les modules complémentaires sont les mêmes pour toutes les offres, sauf pour Availability Monitoring qui est un module complémentaire pour l'offre Cloud APM, Advanced.



Offres

IBM Cloud Application Performance Management, Advanced

Cette offre est conçue pour l'expérience utilisateur final, le suivi des transactions et la surveillance des ressources de tous vos composants d'application. Elle fournit une visibilité du niveau de code dans vos applications et la santé de vos serveurs d'applications. Utilisez les tableaux de bord de diagnostic pour rechercher les goulots d'étranglement des performances dans le code d'application et pour gérer vos applications vitales en production.

L'offre contient IBM Cloud Application Performance Management, Base ainsi que des agents et des collecteurs de données permettant de surveiller des applications, des transactions et d'autres ressources installées dans votre entreprise. Pour une liste des agents et collecteurs de données de cette offre, voir «Fonctions», à la page 40.

Cette offre permet à DevOps de disposer d'une solution complète capable d'offrir la pleine visibilité et le plein contrôle de vos applications et de votre infrastructure. Les propriétaires du secteur d'activité peuvent gérer les applications critiques et l'expérience utilisateur final en production. Les développeurs d'applications peuvent afficher les détails des transactions et diagnostiquer les problèmes des applications.

IBM Cloud Application Performance Management, Base

Cette offre est conçue pour la surveillance de ressources de charges de travail d'infrastructure, de composants d'application et du cloud. La surveillance des ressources vous aide à identifier et traiter les problèmes de transactions lentes, de capacité et d'indisponibilité. L'offre contient des agents et des collecteurs de données permettant de surveiller des applications et d'autres ressources installées dans votre entreprise. Pour une liste des agents et collecteurs de données de cette offre, voir «Fonctions», à la page 40.

Cette offre permet aux opérateurs informatiques de traiter les transactions lentes, les problèmes de capacité et les pannes.

Modules complémentaires

Advanced Extension Pack

Ce module d'extension contient l'Monitoring Agent for SAP HANA Database, l'Agent SAP NetWeaver Java Stack et l'Monitoring Agent for RabbitMQ.

Utilisez l'Agent SAP HANA Database pour surveiller la base de données SAP HANA. Utilisez l'Agent SAP NetWeaver Java Stack pour surveiller SAP NetWeaver Java Stack. Utilisez l'agent RabbitMQ pour surveiller la messagerie RabbitMQ. Ce module d'extension est disponible si vous disposez de l'offre IBM Cloud Application Performance Management, Advanced.

Base Extension Pack

Ce module d'extension contient les agents suivants :

- Monitoring Agent for Cassandra
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for Hadoop
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Internet Service Monitoring

Utilisez ces agents pour surveiller une base de données Cassandra, un cluster Hadoop, des ressources de serveur DataStage, des applications Microsoft Office 365, des serveurs Connect Direct et des applications Sterling File Gateway. Ce module d'extension est disponible si vous disposez de l'une des offres Cloud APM.

Infrastructure Extension Pack

Ce module d'extension contient les agents suivants :

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Citrix Virtual Desktop Infrastructure

Utilisez l'agent Amazon EC2 pour surveiller vos instances Amazon EC2. Utilisez l'agent Amazon ELB pour surveiller vos équilibreurs de charge élastiques AWS. Utilisez l'Agent Azure Compute pour surveiller vos machines virtuelles Azure Compute. Utilisez l'agent Citrix VDI pour surveiller votre infrastructure de bureau virtuel Citrix.

Ce module d'extension est disponible si vous disposez de l'une des offres Cloud APM.

Operations Analytics - Predictive Insights

Ce module complémentaire permet d'analyser les données de mesure qui sont collectées par Cloud APM et de générer des alarmes si des anomalies sont détectées. Le module complémentaire est disponible si vous disposez de l'une des offres Cloud APM.

Pour avoir un aperçu des fonctions disponibles dans chaque offre, voir «Détails d'offre».

Pour obtenir une description de chaque agent et collecteur de données, ainsi que des liens vers les informations spécifiques à chacun, voir «Descriptions», à la page 44.

Détails d'offre

Certaines fonctions sont disponibles dans toutes les offres ; d'autres sont proposées uniquement dans une sélection d'offres.

Le tableau 1, à la page 38 répertorie les principales fonctions disponibles avec chaque offre.

Tableau 1. Fonctions disponibles avec chaque offre

Fonction	Cloud APM, Advanced (Pour DevOps, les développeurs et le secteur d'activité)	Cloud APM, Base (Pour les opérations)
Surveillance des ressources d'application : Langues, middleware (le degré de couverture varie selon l'offre).	✓	✓
Surveillance du système d'exploitation : Systèmes Linux, UNIX et Windows	✓	✓
Surveillance des fichiers journaux : Utilisez les agents de système d'exploitation pour surveiller les fichiers journaux d'application.	✓	✓
Tableaux de bord : • Affichez les indicateurs clés de performance Tivoli Monitoring et Cloud APM dans les mêmes tableaux de bord • Mesures historiques • Tableaux de bords personnalisables	✓	✓
API : Gérez votre environnement à l'aide des API.	✓	✓
Contrôle d'accès basé sur les rôles : Gérez l'accès et les privilèges de vos utilisateurs IBM Cloud Application Performance Management.	✓	✓
Génération de rapports d'historique : Générez des rapports consignant les performances et les temps de réponse de vos applications par transaction, unité, navigateur, etc. (le niveau de couverture varie selon l'offre).	✓	✓
IBM Agent Builder: Créez des agents personnalisés pour surveiller vos différentes plateformes ou technologies.	✓	✓
Surveillance des ressources de base de données : (le degré de couverture varie selon l'offre).	✓	✓
Surveillance des ressources d'infrastructure : Hyperviseurs, stockage et réseau (le degré de couverture varie selon l'offre).	✓	✓
Surveillance des ressources d'applications commerciales : Applications métier et collaboratives (le degré de couverture varie selon l'offre).	✓	✓
Surveillance des temps de réponse : Identifiez en quoi les performances de l'application affectent vos utilisateurs.	✓	✓
Intégration avec l'analyse de recherche : Recherchez des informations approfondies pour isoler, diagnostiquer et résoudre les problèmes rapidement.	✓	✓
Operations Analytics - Predictive Insights (module complémentaire) : Identifiez les anomalies de performance des applications avant qu'elles n'affectent vos utilisateurs.	✓	✓

Tableau 1. Fonctions disponibles avec chaque offre (suite)

Fonction	Cloud APM, Advanced (Pour DevOps, les développeurs et le secteur d'activité)	Cloud APM, Base (Pour les opérations)
Surveillance de l'expérience réelle des utilisateurs : Identifiez les acquis de vos utilisateurs suite à l'utilisation de votre infrastructure sur leur unité.	✓	–
Suivi des transactions : Suivez les transactions de bout en bout au sein de votre environnement d'application. • Topologie d'application : Voyez comment tous les composants sont connectés dans votre environnement d'application. • Topologie des instances de transaction : Visualisez le chemin suivi par chaque instance d'une transaction au sein de votre environnement.	✓	–
Synthetic Playback : Surveillez la disponibilité de vos sites Web internes.	✓	–
Diagnostic approfondi : • Faites une exploration à partir des tableaux de bord récapitulatifs pour afficher des détails sur le niveau de code, les traces de pile et les requêtes SQL concernant des agents spécifiques. • Détectez, diagnostiquez et arrêtez les transactions lentes ou bloquées toujours en cours.	✓	–
Seuils : Détectez des conditions et des comportements d'application spécifiques en fonction de définitions activement surveillées.	✓	✓
Groupes de ressources : Classez les systèmes gérés de votre entreprise surveillée en fonction de leur objet.	✓	✓

Des fonctions supplémentaires, telles que celles décrites ci-dessous, sont disponibles pour toutes les offres par le biais de l'intégration avec d'autres produits et composants. Voir «Intégration», à la page 66 et, pour des informations détaillées, voir Chapitre 11, «Intégration à d'autres produits et composants», à la page 871.)

- Agents Tivoli Monitoring et OMEGAMON : Utilisez la passerelle hybride pour récupérer les données et événements de surveillance pour que ces informations s'affichent dans la console Cloud APM.
- Coexistence des agents : Installez les agents Cloud APM sur le même ordinateur que les agents Tivoli Monitoring.
- Netcool/OMNIbus et autres récepteurs EIF : Transférez les événements à l'IBM Tivoli Netcool/OMNIbus.
- Alert Notification : Recevez une notification lorsque les performances de l'application dépassent les seuils.
- Tivoli Common Reporting
- IBM Cloud : Surveillez les applications IBM Cloud.

Agents et collecteurs de données

Les agents et les collecteurs de données IBM Cloud Application Performance Management sont disponibles à la fois dans les offres et les modules complémentaires.

Nombre de ressources de votre environnement peuvent être surveillées par des agents. Certaines ressources sur IBM Cloud et sur site peuvent être surveillées par des collecteurs de données. Des agents correspondants existent pour tous les collecteurs de données, exceptés les collecteurs de données J2SE et Python. Pour obtenir la liste des agents et des collecteurs de données ainsi que leur description, voir «Descriptions», à la page 44. Pour connaître les fonctions offertes par l'agent ou le collecteur de données pour chaque offre, voir «Fonctions».

Vous pouvez installer ces agents ou collecteurs de données, selon votre environnement et vos exigences. Les collecteurs de données envoient des données directement au serveur Cloud APM. Lorsqu'un agent est configuré, les collecteurs de données lui envoient des données et l'agent les transmet au serveur. Les collecteurs de données fonctionnent dans l'espace des processus d'application, tandis que les agents sont exécutés comme des processus distincts en dehors de l'espace des processus d'application.

Installez des collecteurs de données dans les cas suivants :

- Vous souhaitez une procédure d'installation plus simple.
- Vous utilisez des conteneurs.

Installez des agents dans les cas suivants :

- Vous souhaitez une plus grande évolutivité.
- Vous souhaitez limiter le nombre de sockets des noeuds finals au serveur.
- Lorsque vous ajoutez un seuil dans l'éditeur de seuil, vous souhaitez une liste claire, qui ne contient que les attributs de l'environnement à surveiller. Si vous utilisez un collecteur de données, vous devez sélectionner des attributs de plusieurs collecteurs de données.
- Vous souhaitez activer ou désactiver les fonctions de collecte de données dans l'interface utilisateur, telles que les diagnostics, le suivi des transactions ou la trace de méthode.
- Vous souhaitez afficher les données de diagnostic à la demande, telles que les demandes en cours et le cliché de tas à l'heure actuelle.

Fonctions

Les fonctionnalités d'agent et de collecteur de données varient en fonction de votre offre. Les principales fonctionnalités d'agent et de collecteur de données sont la surveillance des ressources, le suivi des transactions et le diagnostic. Vous pouvez acheter toute offre et module complémentaire de la solution IBM Cloud Application Performance Management . Des offres spécifiques sont requises pour les modules complémentaires.

Chaque agent et collecteur de données surveille les ressources correspondant à son nom ; par exemple, l'Monitoring Agent for Cisco UCS surveille les ressources Cisco UCS.

Selon que vous êtes développeur, dans les opérations, ou propriétaire sectoriel, vous utilisez différentes fonctions d'Cloud APM.

- La fonction de surveillance des ressources inclut la surveillance des temps de réponse, la surveillance des ressources des applications et la surveillance des ressources d'infrastructure. Tous les agents et collecteurs de données peuvent offrir une fonction de surveillance des ressources.
- La fonction de suivi des transactions fournit des informations sur la topologie et l'instance de transaction.
- La fonction de diagnostic inclut le suivi et l'analyse de demandes spécifiques et, si nécessaire, d'appels de méthode.

A faire : La fonction de surveillance des ressources est commune à toutes les offres et tous les modules complémentaires. Les fonctions de diagnostic et de suivi des transactions sont uniquement disponibles dans l'offre Cloud APM, Advanced Private et ses modules complémentaires.

Les agents et les collecteurs de données pour les applications que vous souhaitez surveiller peuvent être téléchargés à partir de Passport Advantage. L'installation des agents prend plusieurs minutes. Les collecteurs de données ne nécessitent pas d'installation, vous devez simplement les configurer une fois le téléchargement terminé. Pour connaître les instructions d'installation des agents, voir Chapitre 9, «Installation des agents», à la page 161.

Le tableau 2 fournit une liste complète des agents et des collecteurs de données, montre quelle offre ou quel module complémentaire contient l'agent ou le collecteur de données, et présente les fonctionnalités de l'agent ou du collecteur de données. Lorsque des modules complémentaires (tels que Infrastructure Extension Pack) sont répertoriés pour un agent ou un collecteur de données, ils sont alors obligatoires. Les agents et les collecteurs de données qui prennent en charge les fonctions de suivi des transactions et/ou de diagnostic sont également indiqués dans la colonne Cloud APM, Advanced Private.

✔ indique que l'agent ou le collecteur de données est disponible dans l'offre et qu'il peut offrir la fonction de surveillance des ressources.

— indique que les données ou la fonction n'est pas disponible dans cette offre, ou que le module complémentaire n'est pas requis pour l'agent ou le collecteur de données.

ST fait référence au suivi des transactions.

DD fait référence au diagnostic.

Tableau 2. Fonctions de l'agent et du collecteur de données dans chaque offre

Agents et collecteurs de données	Cloud APM, Base Private	Cloud APM, Advanced Private	Module complémentaire (si requis)
agent Amazon EC2	✔	✔	Infrastructure Extension Pack
agent Amazon ELB	✔	✔	Infrastructure Extension Pack
Agent Azure Compute	✔	✔	Infrastructure Extension Pack
agent Cassandra	✔	✔	Base Extension Pack
agent Cisco UCS	✔	✔	—
agent Citrix VDI	✔	✔	Infrastructure Extension Pack
Agent Db2	✔	✔	—
agent DataPower	✔	✔ TT	—
Agent DataStage	✔	✔	Base Extension Pack
agent Hadoop	✔	✔	Base Extension Pack

Tableau 2. Fonctions de l'agent et du collecteur de données dans chaque offre (suite)

Agents et collecteurs de données	Cloud APM, Base Private	Cloud APM, Advanced Private	Module complémentaire (si requis)
agent HMC Base	✓	✓	—
agent HTTP Server	✓	✓ TT	—
agent IBM Integration Bus	—	✓ TT (Les services de l'API REST ne sont pas surveillés par l'agent IBM Integration Bus)	—
Internet Service Monitoring	—	—	Base Extension Pack
collecteur de données J2SE pour les applications sur site	—	✓ ST DD	—
agent JBoss	✓	✓ ST DD	—
collecteur de données Liberty pour les applications IBM Cloud et sur site	—	✓ ST DD	—
Agent Linux KVM	✓	✓	—
Agent Linux OS	✓	✓	—
agent Microsoft Active Directory	✓	✓	—
agent Microsoft Cluster Server	✓	✓	—
agent Microsoft Exchange Server	✓	✓	—
agent Microsoft Hyper-V Server	✓	✓	—
agent Microsoft IIS	✓	✓	—
agent Microsoft .NET	✓	✓ ST DD	—
agent Microsoft Office 365	✓	✓	Base Extension Pack
agent Microsoft SharePoint Server	✓	✓	—
agent Microsoft SQL Server	✓	✓ ST DD	—
Agent MongoDB	✓	✓	—
Agent MQ Appliance	—	✓	—
Agent MySQL	✓	✓	—
agent NetApp Storage	✓	✓	—
Agent Node.js	✓	✓ DD	—
collecteur de données Node.js pour les applications IBM Cloud et sur site	—	✓ ST DD	—
Agent OpenStack	✓	✓	—

Tableau 2. Fonctions de l'agent et du collecteur de données dans chaque offre (suite)

Agents et collecteurs de données	Cloud APM, Base Private	Cloud APM, Advanced Private	Module complémentaire (si requis)
Agent Oracle Database	✓	✓	—
Agent PHP	✓	✓	—
Agent PostgreSQL	✓	✓	—
collecteur de données Python pour les applications IBM Cloud et sur site	✓	✓ DD	—
agent RabbitMQ	—	✓	Advanced Extension Pack
Agent de surveillance des temps de réponse	✓	✓ TT	—
Agent Ruby	✓	✓ DD	—
collecteur de données Ruby pour les applications IBM Cloud	—	✓ DD	—
Agent SAP	—	✓	—
Agent SAP HANA Database	—	✓	Advanced Extension Pack
Agent SAP NetWeaver Java Stack	—	✓ ST DD	Advanced Extension Pack
agent Siebel	✓	✓	—
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	✓	✓	—
Agent Sterling Connect Direct	✓	✓	Base Extension Pack
Agent Sterling File Gateway	✓	✓	Base Extension Pack
agent Sybase	✓	✓	—
Agent Synthetic Playback	—	✓	—
Agent Tomcat	✓	✓ TT	—
Agent UNIX OS	✓	✓	—
Agent VMware VI	✓	✓	—
Agent WebLogic	✓	✓ ST DD	—
Agent WebSphere Applications	✓	✓ ST DD	—
Agent WebSphere Infrastructure Manager	✓	✓	—

Tableau 2. Fonctions de l'agent et du collecteur de données dans chaque offre (suite)

Agents et collecteurs de données	Cloud APM, Base Private	Cloud APM, Advanced Private	Module complémentaire (si requis)
Agent WebSphere MQ	–	✓ TT	–
agent Windows OS	✓	✓	–

Pour savoir si la fonction de suivi des transactions ou de diagnostic est activée par défaut pour l'agent ou le collecteur de données, voir le tableau Activation du suivi des transactions pour les agents et les collecteurs de données. Pour plus d'informations sur les tableaux de bord de diagnostic des prédéfinis, voir Tableaux de bord de diagnostic des agents et collecteurs de données.

Descriptions

Les descriptions des agents et des collecteurs de données fournissent des informations sur ce que chacun de ces composants surveille et renvoient vers des informations supplémentaires sur chaque composant.

A chaque agent et collecteur de données est associé un numéro de version qui change chaque fois que l'agent ou le collecteur de données est mis à jour. Dans toute nouvelle édition, des agents et collecteurs de données peuvent être ajoutés et des agents et collecteurs de données existants mis à jour. Si vous ne disposez pas de la dernière version d'un agent ou collecteur de données, prévoyez de le mettre à jour. Pour plus d'informations sur la vérification de la version d'un agent ou d'un collecteur de données dans votre environnement, voir Commande de version d'agent.

Chaque description d'agent et de collecteur de données fournit des liens vers les types de détails suivants relatifs à ces composants :

- Configuration d'agent ou de collecteur de données et autres informations sur des fonctionnalités d'agents ou de collecteurs de données spécifiques
- Fichier PDF de référence qui contient des descriptions des tableaux de bord d'agent ou de collecteur de données, widgets de groupe, seuils, ensembles de données et attributs Cloud APM (mesures et indicateurs clés de performance)

Pour des liens vers la documentation des agents versions 6 et 7 d'IBM Tivoli Monitoring qui peuvent coexister avec des agents et collecteurs de données de Cloud APM version 8, voir tableau 200, à la page 873.

Surveillance d'Amazon EC2

L'Monitoring Agent for Amazon EC2 permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Amazon Elastic Compute Cloud (EC2). Il fournit un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement EC2, y compris l'utilisation de l'UC, l'utilisation d'Elastic Block Store (EBS), l'utilisation du réseau, les mises à jour de maintenance d'Amazon Web Services (AWS) et la performance des disques.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'Amazon EC2», à la page 238.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Amazon EC2 Reference.

Surveillance d'AWS Elastic Load Balancer

L'agent Amazon ELB permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos équilibreurs de charge élastiques AWS. L'agent affiche un ensemble complet de mesures pour chaque type d'équilibreur de charge, application, réseau et classique, qui vous aident à prendre des décisions avisées concernant votre environnement AWS Elastic Load Balancer.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'AWS Elastic Load Balancer», à la page 245.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Amazon ELB Reference.

Surveillance Azure Compute

L'Agent Azure Compute permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Azure Compute. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement Azure Compute. Ces métriques incluent l'utilisation de l'UC, l'utilisation du réseau et les performances du disque.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Azure Compute», à la page 251.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Azure Compute Reference.

Surveillance de Cassandra

L'agent Monitoring Agent for Cassandra vous offre la possibilité de surveiller le cluster Cassandra. Vous pouvez collecter et analyser les informations relatives aux noeuds, espaces de clé et familles de colonnes du cluster Cassandra.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Cassandra», à la page 261.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Cassandra Reference.

Surveillance de Cisco UCS

L'Monitoring Agent for Cisco UCS fournit un environnement permettant de surveiller la santé, le réseau et les performances de Cisco UCS. Il fournit une méthode complète de collecte et d'analyse des informations propres à Cisco UCS qui sont requises pour détecter les problèmes de manière précoce et les éviter.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Cisco UCS», à la page 264.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Cisco UCS Reference.

Surveillance de Citrix Virtual Desktop Infrastructure

L'Monitoring Agent for Citrix Virtual Desktop Infrastructure permet de surveiller de manière centralisée la santé, la disponibilité et les performances de votre infrastructure de postes de travail virtuels Citrix. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant vos ressources XenDesktop ou XenApp, y compris les sites, les machines, les applications, les bureaux, les sessions, les utilisateurs, etc.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Citrix Virtual Desktop Infrastructure», à la page 271.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Citrix VDI Reference.

Surveillance de DataPower

L'Monitoring Agent for DataPower fournit un point central de surveillance des dispositifs DataPower dans votre environnement d'entreprise. Il permet d'identifier et de recevoir des notifications sur les problèmes courants liés aux dispositifs. L'agent fournit également des informations sur les performances, les ressources et la charge de travail des dispositifs.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'agent DataPower», à la page 290.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir DataPower agent Reference.

- Pour plus d'informations sur la surveillance des dispositifs DataPower dans la Pile d'intégration IBM, voir «Surveillance de la Pile d'intégration IBM», à la page 106.

Surveillance de la Db2

L'Monitoring Agent for Db2 offre un point central de surveillance de votre environnement Db2. Il permet de surveiller un grand nombre de serveurs à partir d'une console IBM Performance Management unique, chaque serveur étant surveillé par un agent Db2. Vous pouvez collecter et analyser des informations liées aux applications, bases de données et ressources système.

- Pour obtenir des informations préalablement à la mise à niveau vers une nouvelle version de l'agent, voir «Agents sous AIX : arrêt de l'agent et exécution de **slibclean** avant la mise à niveau», à la page 978
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Db2», à la page 294.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Db2 Reference.
- Pour plus d'informations sur la surveillance des transactions de base de données dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 99.

Surveillance de Hadoop

L'Monitoring Agent for Hadoop fournit à votre organisation des fonctions de surveillance du cluster Hadoop. Il permet de collecter et d'analyser les informations relatives au cluster Hadoop telles que le statut des noeuds de données, les données concernant la machine virtuelle Java, les segments de mémoire et les segments de mémoire non dynamique, les informations sur les noeuds Hadoop, les systèmes de fichiers et les files d'attente.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Hadoop», à la page 305.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Hadoop Reference.

Surveillance de HMC Base

L'Monitoring Agent for HMC Base offre la possibilité de surveiller la console HMC (Hardware Management Console). Il surveille la disponibilité et la santé des ressources HMC : UC, mémoire, stockage et réseau. L'agent génère également des rapports sur l'inventaire et la configuration HMC des serveurs Power, des pools d'UC et des partitions logiques. Les utilisations de l'UC par les serveurs Power, les partitions logiques et les pools sont surveillées à l'aide des exemple de données de performances HMC.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de HMC Base», à la page 314.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent HMC Base Reference.

Surveillance de HTTP Server

L'Monitoring Agent for HTTP Server collecte les données relatives aux performances d'IBM HTTP Server. Par exemple, des informations sur le serveur s'affichent, comme l'état et le type du serveur, le nombre d'erreurs de serveur et de connexions au serveur réussies ou ayant échoué. Un collecteur de données rassemble les données qui sont envoyées à l'agent HTTP Server. Ce dernier s'exécute sur le même système que le serveur IBM HTTP Server qu'il surveille. Chaque serveur surveillé est enregistré en tant que sous-noeud. Le module Temps de réponse IBM HTTP Server est installé avec l'agent HTTP Server. Lorsque vous utilisez l'agent HTTP Server avec l'agent de surveillance Temps de réponse, l'agent WebSphere Application et un agent de base de données, les informations de surveillance des transactions s'affichent dans le navigateur pour la base de données de la pile d'applications IBM Java.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur des systèmes AIX - agent HTTP Server et Préinstallation sur des systèmes Linux agent HTTP Server.

- Pour savoir comment réviser les paramètres du collecteur de données et activer celui-ci après installation de l'agent, voir «Configuration de la surveillance de HTTP Server», à la page 319.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent HTTP Server Reference.
- Pour plus d'informations sur la surveillance des transactions de serveur HTTP dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 99.

Surveillance d'IBM Integration Bus

L'Monitoring Agent for IBM Integration Bus est un outil de surveillance et de gestion qui fournit la possibilité de vérifier, analyser et ajuster les topologies de courtier de messages qui sont associées aux produits IBM WebSphere Message Broker et IBM Integration Bus.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «**Configuration de la surveillance d'IBM Integration Bus**», à la page 323.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent IBM Integration Bus Reference.
- Pour plus d'informations sur la surveillance des courtiers IBM Integration Bus dans la Pile d'intégration IBM, voir «Surveillance de la Pile d'intégration IBM», à la page 106.

Surveillance d'InfoSphere DataStage

L'agent de surveillance d'InfoSphere DataStage surveille la disponibilité, l'utilisation des ressources et les performances du serveur DataStage. Il contrôle l'état de santé des noeuds et des tâches du moteur. Vous pouvez analyser les informations collectées par l'agent et prendre les mesures appropriées pour résoudre les problèmes du serveur DataStage.

- Pour plus d'informations sur la configuration de l'agent après l'installation, voir Configuring InfoSphere DataStage monitoring.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent DataStage Reference.

Internet Service Monitoring

Internet Service Monitoring permet de déterminer si un service particulier fonctionne de manière adéquate, d'identifier les zones problématiques et de générer un rapport sur les performances du service mesurées par rapport aux exigences des contrats de niveau de service (SLA). Internet Service Monitoring fonctionne par émulation des actions d'un utilisateur réel. Il interroge ou teste régulièrement les services Internet pour vérifier leur statut et leurs performances. L'agent Internet Service Monitoring n'est pris en charge que sur les infrastructures sur site.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'agent sur des systèmes Windows», à la page 415.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document Internet Service Monitoring Agent Reference

Surveillance du collecteur de données J2SE

Le collecteur de données J2SE collecte les données de surveillance des ressources et de diagnostics approfondis pour les applications Java. Les données de diagnostic approfondi sont affichées dans les tableaux de bord en fonction des demandes et des informations globales pour prendre en charge diverses vues d'exploration. La surveillance des ressources et le diagnostic approfondi sont pris en charge, ce qui permet de détecter, isoler et diagnostiquer les problèmes de vos applications Java. Vous pouvez configurer le collecteur de données pour diagnostiquer les demandes lentes.

- Pour plus d'informations sur la configuration du collecteur de données, voir Configuration du collecteur de données J2SE.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document J2SE data collector Reference.

Surveillance de JBoss

L'Monitoring Agent for JBoss surveille les ressources des serveurs d'applications JBoss et de la plateforme JBoss Enterprise Application. Utilisez les tableaux de bord fournis avec l'agent JBoss pour identifier les applications et les demandes les plus lentes, les goulots d'étranglement dans le pool d'unités d'exécution, les problèmes de segment de mémoire JVM et de récupération de place, les sessions les plus actives et les autres goulots d'étranglement sur le serveur d'applications JBoss.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de JBoss», à la page 423.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent JBoss Reference.

Surveillance de Linux KVM

L'Monitoring Agent for Linux KVM est un agent multi-instance et multiconnexion qui prend en charge des connexions d'hyperviseur KVM basé sur Enterprise Linux et des environnements RHEVM (Red Hat Enterprise Virtualization Manager). Vous pouvez créer plusieurs instances de cet agent pour surveiller plusieurs hyperviseurs dans un environnement d'hyperviseur RHEV-M ou KVM. Vous pouvez surveiller les charges de travail virtualisées et analyser la capacité de ressources sur des machines virtuelles différentes. Pour connecter l'agent à une machine virtuelle dans l'environnement de l'hyperviseur KVM, vous devez installer les conditions préalables requises : `libvirt*.rpm` et interpréteur de commandes Korn (pdksh). L'agent collecte des indicateurs en se connectant à distance à un hyperviseur libvirt qui gère les machines virtuelles.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Linux KVM», à la page 439.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Linux KVM Reference.

Surveillance de Linux OS

L'Monitoring Agent for Linux OS fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de l'environnement de système d'exploitation Linux. Cet agent prend en charge la surveillance du conteneur de docker. Par exemple, des informations détaillées sur l'utilisation de l'UC, de la mémoire, du réseau et des E/S liées au conteneur de docker s'affichent. Des informations générales sur les conteneurs de docker exécutés sur le serveur, telles que l'ID et le nom d'instance du docker, s'affichent également. En outre, vous pouvez configurer la surveillance des fichiers journaux afin de surveiller les fichiers journaux d'application. Vous pouvez collecter et analyser des informations propres au serveur, comme les performances du système d'exploitation et de l'UC, l'analyse des informations et des performances du disque Linux, l'analyse de l'état des processus et les performances réseau.

- Pour des informations sur la configuration de la surveillance des fichiers journaux après l'installation, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 590.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Linux OS Reference.

Surveillance de Microsoft Active Directory

L'Monitoring Agent for Microsoft Active Directory fournit à votre organisation des fonctions de surveillance d'Active Directory. Il permet de collecter et d'analyser les informations propres à Active Directory, comme l'état du réseau, la réplication Sysvol, les performances du carnet d'adresses et l'utilisation du système d'annuaire.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Active Directory», à la page 450.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Active Directory Reference.

Surveillance de Microsoft Cluster Server

L'Monitoring Agent for Microsoft Cluster Server fournit à votre organisation des fonctions de

surveillance de Microsoft Cluster Server. Il permet de collecter les informations liées à la disponibilité des ressources de cluster, comme le niveau du cluster, les noeuds du cluster, les groupes de ressources du cluster, les ressources du cluster et les réseaux du cluster. Il fournit également des statistiques sur l'utilisation des ressources du cluster, comme l'utilisation du processeur, de la mémoire, du disque et du réseau.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Cluster Server», à la page 455.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Monitoring Agent for Microsoft Cluster Server Reference.

Surveillance de Microsoft Exchange Server

L'Monitoring Agent for Microsoft Exchange Server offre à votre organisation des fonctions de surveillance de la santé, de la disponibilité et des performances des serveurs Exchange Server. Vous pouvez utiliser l'agent Microsoft Exchange Server pour collecter des informations propres au serveur, comme le trafic via la messagerie, l'état des bases de données de boîte aux lettres et les activités des clients. Il fournit également des statistiques sur l'utilisation du cache, de la messagerie et de la base de données et sur les activités des clients pour vous aider à analyser les performances des serveurs Exchange Server.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Exchange», à la page 457.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Exchange Server Reference.

Surveillance de Microsoft Hyper-V Server

L'Monitoring Agent for Microsoft Hyper-V Server offre à votre organisation la possibilité de surveiller la disponibilité et les performances de tous les systèmes Hyper-V. Il fournit des informations de configuration comme le nombre et l'état des machines virtuelles, le nombre de disques virtuels alloués, la mémoire virtuelle allouée et le nombre de processeurs virtuels alloués. Il fournit également des statistiques sur l'utilisation du processeur physique, de la mémoire, du réseau, du processeur logique et du processeur virtuel.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Hyper-V», à la page 471.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Hyper-V Server Reference.

Surveillance de Microsoft Internet Information Services

L'Monitoring Agent for Microsoft Internet Information Services vous offre la possibilité de surveiller la disponibilité et les performances de Microsoft Internet Information Server. Vous pouvez utiliser l'agent Microsoft Internet Information Server pour surveiller les détails d'un site Web, comme le taux des demandes, la vitesse de transfert des données et les statistiques sur les erreurs et les connexions.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft IIS», à la page 475.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft IIS Reference.

Surveillance de Microsoft .NET

L'Monitoring Agent for Microsoft .NET surveille les applications Microsoft .NET qui sont basées sur Internet Information Services (IIS) et les ressources Microsoft .NET Framework. Le composant de collecteur de données collecte les données des demandes HTTP entrantes. Il collecte les appels de méthode, construit une arborescence d'appels et collecte le contexte des demandes et les données de trace de pile. Utilisez les tableaux de bord fournis avec l'agent Microsoft .NET pour identifier les problèmes liés à Microsoft .NET Framework et les demandes HTTP les plus lentes à partir desquelles vous pouvez explorer les informations de trace de pile pour isoler les problèmes.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Enregistrement du collecteur de données», à la page 485.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft .NET Reference.

Surveillance de Microsoft Office 365

L'agent Monitoring Agent for Microsoft Office 365 vous offre la possibilité de surveiller Microsoft Office 365. Vous pouvez collecter et analyser les informations relatives à Microsoft Exchange Online, SharePoint Online, Skype for Business et OneDrive for Business.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Office 365», à la page 494.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Office 365 Reference.

Surveillance de Microsoft SharePoint Server

L'Monitoring Agent for Microsoft SharePoint Server vous offre l'environnement permettant de surveiller la disponibilité, les événements et les performances de Microsoft SharePoint Server. Utilisez cet agent pour collecter des données à partir de Microsoft SharePoint Server et pour gérer les opérations.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft SharePoint Server», à la page 500.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Monitoring Agent for Microsoft SharePoint Server Reference.

Surveillance de Microsoft SQL Server

L'agent Monitoring Agent for Microsoft SQL Server vous offre la possibilité de surveiller Microsoft SQL Server. L'agent Microsoft SQL Server offre un point de gestion centralisé des bases de données réparties. Utilisez les tableaux de bord de l'agent Microsoft SQL Server pour surveiller la disponibilité, les performances, l'utilisation des ressources et l'état général de toutes les instances SQL Server surveillées.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft SQL Server», à la page 504.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft SQL Server Reference.

Surveillance de MongoDB

L'Monitoring Agent for MongoDB fournit des fonctions de surveillance de l'utilisation, de l'état et des performances du déploiement MongoDB. Vous pouvez collecter et analyser des informations comme l'utilisation de la capacité de la base de données, le pourcentage de connexions ouvertes, l'utilisation de la mémoire, l'état de l'instance et le temps de réponse dans des tableaux de bord visualisés.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de MongoDB», à la page 533.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent MongoDB Reference.

Surveillance de MQ Appliances

Monitoring Agent for MQ Appliance fournit des informations sur la surveillance axées sur le niveau de MQ Appliances, telles que des informations récapitulatives sur l'UC, la mémoire, le stockage, les capteurs et les gestionnaires de files d'attente.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'IBM MQ Appliances», à la page 335.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document MQ Appliance agent Reference.

Surveillance de MySQL

L'Monitoring Agent for MySQL fournit des fonctions de surveillance de l'état, de l'utilisation et des performances du déploiement MySQL. Vous pouvez collecter et analyser des informations comme Octets reçus / envoyés, Pages du pool de mémoire tampon InnoDB et Historique des performances.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur des systèmes Linux - Agent MySQL ou Préinstallation sur des systèmes Windows - Agent MySQL.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de MySQL», à la page 539.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent MySQL Reference.

Surveillance de NetApp Storage

L'Monitoring Agent for NetApp Storage vous permet de surveiller les systèmes de stockage NetApp à l'aide de NetApp OnCommand Unified Manager (OCUM). Vous pouvez collecter et analyser les informations relatives aux agrégats, aux noeuds, aux disques et aux volumes des systèmes de stockage NetApp.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de NetApp Storage», à la page 542.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent NetApp Storage Reference.

Surveillance de Node.js

L'Monitoring Agent for Node.js ou le collecteur de données Node.js autonome peut être utilisé pour mesurer et collecter des données sur les performances des applications Node.js. Par exemple, la capacité de traitement et les temps de réponse pour les demandes HTTP, ainsi que d'autres mesures liées à l'utilisation des ressources, sont surveillés et stockés à des fins d'affichage et d'analyse. Pour choisir entre l'Agent Node.js et le collecteur de données Node.js, reportez-vous à la rubrique «Configuration de la surveillance de Node.js», à la page 548 pour des instructions.

Agent Node.js

- Avant de commencer l'installation, voir Préinstallation sur des systèmes Linux - Agent Node.js.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'Agent Node.js», à la page 549.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Node.js Reference.

collecteur de données Node.js (autonome)

Le collecteur de données Node.js surveille les applications IBM Cloud et sur site. La surveillance des ressources et le diagnostic approfondi sont pris en charge, ce qui permet de détecter, isoler et diagnostiquer les problèmes de vos applications. Vous pouvez configurer le collecteur de données pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 555.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collector Reference.

Applications sur site

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 561.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collector Reference.

Surveillance d'OpenStack

L'Monitoring Agent for OpenStack vous permet de surveiller vos applications OpenStack. Utilisez les tableaux de bord pour visualiser les performances de vos applications OpenStack, telles que les informations sur les noeuds finals d'API, la connexion au serveur SSH, les processus et les hyperviseurs.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'Agent OpenStack», à la page 568.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent OpenStack Reference.

Surveillance d'Oracle Database

L'Monitoring Agent for Oracle Database fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de la base de données Oracle. Vous pouvez configurer plusieurs instances d'Agent Oracle Database pour surveiller différentes bases de données Oracle. La fonction de surveillance à distance est également fournie par cet agent.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur des systèmes AIX - Agent Oracle Database, Préinstallation sur des systèmes Linux - Agent Oracle Database ou Préinstallation sur des systèmes Windows - Agent Oracle Database (Windows).
- Pour savoir comment configurer l'agent après installation, voir «Configuration de la surveillance d'Oracle Database», à la page 573.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Oracle Database Reference.
- Pour plus d'informations sur la surveillance des transactions de base de données dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 99.

Surveillance de PHP

L'Monitoring Agent for PHP surveille les applications Web PHP en collectant les indicateurs d'accès au Web via un serveur Web Apache et des données de statistiques de performances à partir de MySQL. L'agent reconnaît toutes les applications WordPress sur un serveur Apache et fournit des informations statistiques sur l'application WordPress. Il permet de surveiller la disponibilité du serveur Web, l'état du serveur Apache et les demandes GET/POST. L'agent évalue uniquement les performances des requêtes PHP dans les applications WordPress. Le chargement CSS et JS n'est pas évalué. L'agent n'utilise pas les arguments d'URL pour identifier les URL.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de PHP», à la page 617.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent PHP Reference.

Surveillance de PostgreSQL

L'Monitoring Agent for PostgreSQL surveille la base de données PostgreSQL en collectant des indicateurs PostgreSQL via un pilote JDBC. Il fournit des données sur l'utilisation des ressources système, la capacité de la base de données, les connexions utilisées, l'état individuel des instances en cours d'exécution, les statistiques sur les opérations, le temps de réponse pour les instructions de requête SQL, les détails de taille de la base de données et les informations de verrou.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance PostgreSQL», à la page 619.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent PostgreSQL Reference.

Surveillance de Python

Le collecteur de données Python surveille à la fois les applications Python sur site et IBM Cloud. La surveillance des ressources et le diagnostic approfondi sont tous deux pris en charge, ce qui génère des données de surveillance, telles que la quantité d'UC et de mémoire utilisée, la récupération de place et les unités d'exécution. Vous pouvez configurer le collecteur de données pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 624.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Data collector Reference.

Applications sur site

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Python pour les applications sur site», à la page 629.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Data collector Reference.

Surveillance de RabbitMQ

L'Monitoring Agent for RabbitMQ vous offre la possibilité de surveiller le cluster RabbitMQ. Vous pouvez collecter et analyser les informations relatives aux noeuds, files d'attente et chaînes du cluster RabbitMQ.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de RabbitMQ», à la page 635.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent RabbitMQ Reference.

Surveillance des temps de réponse

Agent de surveillance des temps de réponse utilise la surveillance du réseau pour capturer les données de transaction HTTP et HTTPS, telles que les temps de réponse et les codes de statut. Il permet de surveiller les performances et la disponibilité des applications Web pour les utilisateurs, y compris les informations relatives aux demandes de transaction, à l'application et aux serveurs. Utilisez également cet agent pour surveiller les périphériques et les informations de session.

- Avant de commencer l'installation de l'Agent de surveillance des temps de réponse, voir Préinstallation sur des systèmes AIX - Agent de surveillance des temps de réponse, Préinstallation sur des systèmes Linux - Agent de surveillance des temps de réponse ou Préinstallation sur des systèmes Windows - Agent de surveillance des temps de réponse.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Injection JavaScript», à la page 642.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Transaction Monitoring Reference.
- Pour plus d'informations sur l'utilisation de la Surveillance des temps de réponse dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 99.

Surveillance de Ruby

L'Monitoring Agent for Ruby ou les collecteurs de données Ruby autonomes surveillent les performances de vos applications Ruby on Rails, comprenant le trafic des demandes et les statistiques sur la configuration. Vous pouvez également utiliser la fonction de diagnostic pour obtenir une vue plus précise de chaque application.

Le collecteur de données Ruby autonome surveille uniquement les applications IBM Cloud.

Agent Ruby

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Ruby», à la page 669.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Ruby Reference.

collecteur de données Ruby (autonome)

Vous pouvez utiliser le collecteur de données Ruby pour surveiller les applications IBM Cloud. La surveillance des ressources et le diagnostic approfondi sont tous deux pris en charge, ce qui permet de détecter, isoler et diagnostiquer les problèmes de vos applications. Vous pouvez configurer le collecteur de données pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir Configuration du collecteur de données Ruby.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collector Reference.

Surveillance des applications SAP

L'Monitoring Agent for SAP Applications vous offre la possibilité de surveiller vos applications SAP qui fonctionnent sur la pile Advanced Business Application Programming (ABAP). L'agent surveille également SAP Solution Manager, qui est un outil de gestion du cycle de vie SAP, et SAP NetWeaver Process Integration (SAP PI), qui est un logiciel d'intégration d'entreprise pour SAP. Il offre un point central de gestion pour la collecte des informations dont vous avez besoin pour détecter les problèmes de manière précoce et suivre la procédure nécessaire pour les éviter à nouveau. Il permet une gestion efficace des systèmes, quels que soient les modules, les applications et les versions de SAP, ainsi que les bases de données, systèmes d'exploitation et interfaces externes utilisés.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de SAP», à la page 681.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent SAP Reference.

Surveillance de SAP HANA Database

L'Monitoring Agent for SAP HANA Database surveille la disponibilité, l'utilisation des ressources et la performance de la base de données HANA SAP. L'agent peut surveiller les scénarios de déploiement HANA tels que hôte unique - base données unique, hôte unique - bases de données titulaires multiples, hôtes multiples - base de données unique et hôtes multiples - bases de données titulaires multiples. Vous pouvez analyser les informations que l'agent collecte et prendre des mesures appropriées pour résoudre des problèmes dans la base de données HANA SAP.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur les systèmes AIX - Agent SAP HANA Database ou Préinstallation sur les systèmes Linux - Agent SAP HANA Database ou Préinstallation sur les systèmes Windows - Agent SAP HANA Database.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de SAP HANA Database», à la page 699.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent SAP HANA Database Reference.

Surveillance de SAP NetWeaver Java Stack

L'Monitoring Agent for SAP NetWeaver Java Stack surveille la disponibilité, l'utilisation des ressources et les performances de SAP NetWeaver Java Stack. L'agent peut surveiller les scénarios de déploiement SAP NetWeaver Java Stack tels que hôte unique - instance unique, hôte unique - instances multiples, hôtes multiples - instances uniques et hôtes multiples - instances multiples.

Vous pouvez analyser les informations collectées par l'agent et prendre des mesures appropriées pour résoudre des problèmes dans SAP NetWeaver Java Stack.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 701.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent SAP NetWeaver Java Stack Reference.

Surveillance de Siebel

L'Monitoring Agent for Siebel permet de surveiller de manière centralisée vos ressources Siebel, notamment les statistiques Siebel, les sessions utilisateur, les composants, les tâches, le serveur d'application, le serveur de noms de passerelle Siebel, l'utilisation de la mémoire et de l'UC de processus et la surveillance des événements du journal.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Siebel», à la page 708.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Siebel Reference.

Surveillance Skype for Business Server (anciennement Microsoft Lync Server)

L'Monitoring Agent for Skype for Business Server vous permet de surveiller la santé, la disponibilité et les performances de Skype for Business Server. Vous pouvez utiliser l'agent Skype for Business Server pour collecter des informations spécifiques au serveur, telles que le temps d'attente, les transactions synthétiques, les opérations d'écriture de service d'enregistrement de détail d'appel (CDR), l'état des demandes régulées et les homologues SIP. De plus, l'agent fournit des statistiques d'utilisation historiques de la messagerie instantanée et du serveur de médiation pour vous aider à analyser les performances des serveurs Lync ou Skype for Business.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Skype for Business Server (anciennement Microsoft Lync Server)», à la page 478.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Skype for Business Server Reference.

Surveillance Sterling Connect Direct

L'Monitoring Agent for Sterling Connect Direct permet de surveiller la santé et les performances des serveurs Connect Direct. Il fournit également une analyse de l'activité de transfert de fichiers.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Sterling Connect Direct», à la page 719.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Sterling Connect Direct Reference.

Surveillance Sterling File Gateway

L'Monitoring Agent for Sterling File Gateway surveille l'application Sterling File Gateway, utilisée pour transférer des fichiers entre les partenaires internes et externes à l'aide de différents protocoles, différentes conventions de dénomination de fichier et différents formats de fichier. Il prend également en charge la fonction de surveillance à distance.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Sterling File Gateway», à la page 722.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Sterling File Gateway Reference.

Surveillance Sybase Server

L'Monitoring Agent for Sybase Server offre un point central de gestion pour les bases de données distribuées. Il collecte les informations requises pour que les administrateurs de base de données et système puissent examiner les performances du système Sybase Server, détecter rapidement les problèmes et les empêcher.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Sybase Server», à la page 728.

- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir l'agent Sybase Reference.

Surveillance de Synthetic Playback

L'Monitoring Agent for Synthetic Playback surveille la disponibilité et les performances des applications internes et externes. Enregistrez les scripts de test à l'aide de Selenium IDE et téléchargez vos scripts pour créer des transactions synthétiques pour vos applications. Pour répliquer votre expérience utilisateur, vous pouvez réexécuter vos transactions synthétiques à des intervalles différents et à plusieurs emplacements. Visualisez les mesures relatives au statut et aux performances des transactions synthétiques sur les tableaux de bord. Exécutez des rapports afin de visualiser les données relatives aux performances historiques de vos applications.

L'Monitoring Agent for Synthetic Playback diffère des autres agents Cloud APM dans le sens où il envoie des données au serveur Cloud APM. L'Agent Synthetic Playback n'envoie aucune donnée de diffusion directement au serveur Cloud APM. Il envoie des données JSON à une plateforme Kafka. Celles-ci sont ensuite stockées dans la base de données MongoDB. Un fournisseur de données personnalisées envoie des attributs calculés de la base de données MongoDB aux widgets de Tableau de bord d'Application Performance pour les transactions synthétiques.

L'Agent Synthetic Playback n'utilise pas l'infrastructure de surveillance des seuils et des événements Cloud APM. La prise en charge des seuils dans le cadre l'Agent Synthetic Playback est fournie par l'agent Synthetic Events qui s'exécute du côté du serveur Cloud APM. Pour plus d'informations, voir «Gestion des événements synthétiques», à la page 1068.

- Avant de commencer l'installation, voir Préinstallation sur des systèmes Linux - Agent Synthetic Playback.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Synthetic Playback», à la page 734.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Synthetic Playback Reference.

Surveillance de Tomcat

L'Monitoring Agent for Tomcat surveille les ressources des serveurs d'applications Tomcat. Utilisez les tableaux de bord fournis avec l'agent Tomcat pour identifier les applications et les demandes les plus lentes, les goulots d'étranglement dans le pool d'unités d'exécution, les problèmes de segment de mémoire JVM et de récupération de place, les sessions les plus actives et les autres goulots d'étranglement sur le serveur d'applications Tomcat.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Tomcat», à la page 735.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Tomcat Reference.

Surveillance d'UNIX OS

L'Monitoring Agent for UNIX OS fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de l'environnement de système d'exploitation UNIX. (système d'exploitation AIX uniquement. Voir System requirements dans APM Developer Center.) En outre, vous pouvez configurer la surveillance des fichiers journaux afin de surveiller les fichiers journaux d'application. Vous pouvez collecter et analyser des informations propres au serveur, comme les performances du système d'exploitation et de l'UC, l'analyse des informations sur le disque UNIX et des performances, l'analyse de l'état des processus et les performances réseau.

- Pour des informations sur la configuration de la surveillance des fichiers journaux après l'installation, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 590.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent UNIX OS Reference.

Surveillance de VMware VI

L'Monitoring Agent for VMware VI surveille l'infrastructure virtuelle VMware en se connectant au centre virtuel VMware. Il permet d'afficher le récapitulatif d'état des clusters et de surveiller plusieurs composants, tels que les clusters, les machines virtuelles, les magasins de données et les serveurs ESX à partir d'une console unique.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de VMware VI», à la page 741.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent VMware VI Reference.

Surveillance de WebLogic

L'Monitoring Agent for WebLogic permet de surveiller de manière centralisée la santé, la disponibilité et les performances de votre environnement de serveur WebLogic. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant vos ressources WebLogic, y compris les machines virtuelles Java, le service de messagerie Java et la connectivité Java Database Connectivity (JDBC).

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de WebLogic», à la page 750.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent WebLogic Reference.

Surveillance des applications WebSphere

L'Monitoring Agent for WebSphere Applications avec le collecteur de données imbriqué ou le collecteur de données Liberty autonome surveille les ressources des serveurs WebSphere Application Server. Ces composants de surveillance peuvent être configurés pour effectuer les opérations suivantes :

- Ils collectent les indicateurs PMI de surveillance des ressources via une interface JMX sur le serveur d'applications.
- Ils collectent les métriques de performances des demandes agrégées.
- Ils suivent les performances des appels de demande et de méthode individuels.

Les données de surveillance sont affichées dans les tableaux de bord. Vous pouvez utiliser les tableaux de bord fournis pour isoler les zones problématiques de votre serveur d'applications. Effectuez une exploration en aval pour déterminer si un problème est lié à une ressource sous-jacente ou au code de l'application.

Pour déterminer si l'agent ou l'un des collecteurs de données doit être utilisé, voir «Configuration de la surveillance des applications WebSphere», à la page 765.

Agent et collecteur de données imbriqué des applications WebSphere

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration du collecteur de données pour l'Agent WebSphere Applications», à la page 766.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent WebSphere Applications Reference.
- Pour plus d'informations sur la surveillance des transactions WebSphere Application Server dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 99.

Collecteur de données Liberty (autonome)

Vous pouvez utiliser le collecteur de données Liberty pour surveiller le profil WebSphere Liberty sur IBM Cloud ou surveiller WebSphere Application Server Liberty on Linux for System x. La surveillance des ressources, les diagnostics et le suivi des transactions sont tous pris en charge, ce qui permet de détecter, d'isoler et de diagnostiquer les problèmes de vos applications. Vous pouvez configurer le collecteur de données autonome pour le

suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 845.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document Liberty data collector Reference.

Applications sur site (Linux for System x uniquement)

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Liberty pour les applications sur site», à la page 813.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document Liberty data collector Reference.

Surveillance de WebSphere Infrastructure Manager

L'Monitoring Agent for WebSphere Infrastructure Manager fournit les fonctionnalités de surveillance de WebSphere Application Server Deployment Manager et de l'agent de noeud, avec notamment le statut du serveur, les ressources et les transactions. Vous pouvez utiliser les données collectées par l'agent WebSphere Infrastructure Manager pour analyser les performances de votre gestionnaire de déploiement et de l'agent de noeud et déterminer si un problème s'est produit.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de WebSphere Infrastructure Manager», à la page 852.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent WebSphere Infrastructure Manager Reference.

Surveillance de WebSphere MQ

Avec l'Monitoring Agent for WebSphere MQ, vous pouvez aisément collecter et analyser les données propres à WebSphere MQ pour vos gestionnaires de files d'attente à partir d'un point d'observation unique. Vous pouvez alors suivre les tendances dans les données collectées et traiter les problèmes système à l'aide des tableaux de bord prédéfinis.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de WebSphere MQ», à la page 853.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent WebSphere MQ Reference.
- Pour plus d'informations sur la surveillance des files d'attente de message dans la Pile d'intégration IBM, voir «Surveillance de la Pile d'intégration IBM», à la page 106.

Surveillance de Windows OS

L'Monitoring Agent for Windows OS fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de l'environnement de système d'exploitation Windows. En outre, vous pouvez configurer la surveillance des fichiers journaux afin de surveiller les fichiers journaux d'application. Vous pouvez collecter et analyser des informations propres au serveur, comme les performances du système d'exploitation et de l'UC, l'analyse des informations sur le disque et des performances, l'analyse de l'état des processus, les données de session Internet, les informations des journaux surveillés, les statistiques sur le serveur Internet, les statistiques sur la mise en file d'attente des messages, les données d'état d'imprimante et de travail, les statistiques Remote Access Services et les informations relatives aux services. Le service KNTCMA_FCProvider est installé avec l'agent.

- Pour des informations sur la configuration de la surveillance des fichiers journaux après l'installation, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 590.

- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Windows OS Reference.

Fonctions

Les fonctions principales varient selon l'offre utilisée. Certaines fonctions sont disponibles dans une seule ou dans les deux offres, dans un module complémentaire ou encore par le biais de l'intégration à d'autres produits et composants.

Surveillance des ressources d'application
Utilisez les agents de surveillance des ressources pour surveiller les langues et les middleware. La couverture varie selon l'offre. Voir «Fonctions», à la page 40.

Surveillance du système d'exploitation
Utilisez les agents de surveillance des ressources pour surveiller les systèmes d'exploitation Linux, UNIX et Windows. Voir «Fonctions», à la page 40.

Surveillance des fichiers journaux
Les agents de système d'exploitation incluent une fonction pour surveiller les fichiers journaux d'application. Cette fonction permet de configurer la surveillance des fichiers journaux sur la base d'expressions régulières.

Pour des raisons de compatibilité, l'agent de système d'exploitation utilise les informations et les formats suivants :

- Les informations de configuration et le fichier de format utilisé par IBM Tivoli Monitoring Log File Agent V6.x
- Les informations de configuration et les chaînes de format utilisées par Tivoli Event Console Log File Adapter

Ces chaînes de format permettent à l'agent de filtrer les données de journal en fonction de masques dans le fichier de format et de soumettre uniquement les données appropriées à un consommateur d'événement. L'agent de système d'exploitation envoie des données au serveur Cloud APM ou via EIF (Event Integration Facility) à un récepteur EIF, comme Netcool/OMNIbus Probe for Tivoli EIF.

Tableaux de bord
Le **Tableau de bord d'Application Performance** fournit le statut général des applications dans votre environnement. Visualisez les domaines qui vous intéressent en les sélectionnant dans le navigateur ou en cliquant dans une zone récapitulative pour accéder au niveau suivant.

Pour en savoir plus sur les fonctionnalités disponibles à chaque niveau du tableau de bord, voir «Toutes mes applications - Tableau de bord d'Application Performance», à la page 1125, «Application - Tableau de bord d'Application Performance», à la page 1128 et «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1133.

Affichez les indicateurs clés de performance des domaines Tivoli Monitoring et Cloud APM dans les mêmes tableaux de bord
Dans un environnement qui inclut les produits IBM Tivoli Monitoring et IBM Cloud Application Performance Management, vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management afin d'offrir une vue consolidée des systèmes gérés provenant des deux domaines. Pour afficher votre environnement hybride dans la console Cloud APM, vous devez créer un groupe de systèmes gérés, installer la Passerelle hybride dans votre environnement Tivoli Monitoring et configurer les communications avec la Passerelle hybride.

Pour plus d'informations, voir «Intégration à IBM Tivoli Monitoring V6.3», à la page 871.

Mesures historiques
Visualisez jusqu'à 24 heures de données historiques sur les Tableau de bord d'Application Performance. Si une barre de sélection de durée s'affiche dans l'onglet **Présentation des**

statuts d'un tableau de bord, vous pouvez ajuster la période des graphiques et les tableaux dont les valeurs sont dérivées des échantillons de données historiques. Pour les graphiques à courbes, vous pouvez également comparer les données actuelles, jusqu'aux dernières 24 heures, avec jusqu'à 8 jours de données historiques pour déceler les anomalies.

Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1138.

Vue universelle d'IBM Cloud Application Business Insights

Vous pouvez utiliser la Vue universelle pour créer des pages personnalisées pour les applications que vous surveillez. Vous avez le choix entre plusieurs options de graphique et de mesure pour créer des widgets permettant de surveiller les données en fonction de vos besoins. Avec la Vue universelle, vous pouvez personnaliser un tableau de bord pour afficher les données consolidées de plusieurs agents.

Lorsque vous affichez les données dans le tableau de bord, vous pouvez modifier dynamiquement le type du graphique. Dans le widget de grille, vous pouvez filtrer les données de manière dynamique.

Vous pouvez exporter les données de pages personnalisées dans un fichier de données brutes.

Pour plus d'informations, voir «Vues personnalisées», à la page 1160.

Détails d'application

Lorsque vous accédez à un tableau de bord détaillé d'une instance de système géré à partir du tableau de bord Toutes mes applications, l'onglet Détails d'attribut s'affiche pour vous permettre de créer et de gérer des graphiques à courbes d'historique et des tableaux personnalisés pouvant être sauvegardés. Vous pouvez sauvegarder des pages de graphiques ou de tableaux supplémentaires pour affichage uniquement ou à des fins de partage avec tous les utilisateurs du même environnement.

Pour plus d'informations, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1140.

API Les API Cloud APM sont disponibles pour gérer votre environnement, par exemple pour affecter des rôles d'utilisateurs et créer des seuils. Pour plus d'informations, voir «Exploration des API», à la page 1115.

Contrôle d'accès basé sur les rôles

Dans Cloud APM, un rôle est un groupe de droits d'accès qui contrôlent les actions que vous pouvez effectuer. La fonction Contrôle d'accès basé sur les rôles permet de créer des rôles personnalisés. Les quatre rôles prédéfinis suivants sont disponibles : Administrateur de rôles, Administrateur de surveillance, Administrateur système et Utilisateur de surveillance. Vous pouvez affecter aux utilisateurs à la fois des rôles personnalisés et des rôles prédéfinis et les utilisateurs peuvent être affectés à plusieurs rôles. Vous pouvez affecter des droits à des rôles personnalisés ou davantage de droits aux rôles par défaut existants. Les droits d'accès sont cumulatifs. Un utilisateur dispose de tous les droits de tous les rôles auxquels ils sont affectés.

Vous pouvez affecter des droits d'affichage et de modification à des applications individuelles, des groupes de ressources système et des groupes de ressources personnalisées. Par exemple, si vous êtes membre d'un rôle doté du droit d'affichage pour une application, vous pouvez afficher tous les composants de prise en charge dans cette application.

Vous pouvez affecter des droits d'affichage et de modification à des tâches d'administration de système. Par exemple, si vous êtes membre d'un rôle doté du droit d'affichage de la configuration avancée, vous pouvez effectuer et sauvegarder des modifications dans la fenêtre Configuration avancée.

Pour plus d'informations, voir «Rôles et droits», à la page 1021.

Génération de rapports d'historique
Les rapports sont disponibles pour les données collectées par l'Agent WebSphere Applications, l'Agent de surveillance des temps de réponse et l'Agent Synthetic Playback. Le suivi des transactions est obligatoire pour les rapports de l'Agent de surveillance des temps de réponse (non disponibles avec Cloud APM, Base Private) Pour plus d'informations sur l'installation des rapports, voir «Intégration à Tivoli Common Reporting», à la page 917. Pour des descriptions de rapport, voir «Rapports», à la page 1172.

Si vous avez un environnement IBM Tivoli Monitoring qui est configuré avec Tivoli Data Warehouse, vous pouvez envoyer des données des agents Cloud APM vers l'entrepôt de données pour utilisation dans des rapports de Tivoli Common Reporting.

Agent Builder
Créez des agents personnalisés pour surveiller vos différentes plateformes ou technologies. Voir Guide d'utilisation d'IBM Agent Builder.

Surveillance des ressources de base de données
La couverture varie selon l'offre. Voir «Fonctions», à la page 40 pour afficher les noms des bases de données pouvant être surveillées.

Surveillance des ressources d'infrastructure
Utilisez les agents de surveillance des ressources pour surveiller les hyperviseurs, le stockage et les réseaux. La couverture varie selon l'offre. Voir «Fonctions», à la page 40.

Surveillance des ressources d'applications commerciales
Utilisez les agents de surveillance des ressources pour surveiller les applications métier et collaboratives. La couverture varie selon l'offre. Voir «Fonctions», à la page 40.

Surveillance des temps de réponse et de l'expérience de l'utilisateur
Identifiez les acquis de vos utilisateurs suite à l'utilisation de votre infrastructure sur leur périphérique. Utilisez la surveillance des temps de réponse pour surveiller les performances et la disponibilité des sites et applications Web à partir du navigateur via la base de données, et pour surveiller des périphériques mobiles. Une fois que vous avez installé l'Agent de surveillance des temps de réponse sur les serveurs à surveiller, les données collectées par ces agents sont affichées dans le Tableau de bord d'Application Performance (aucune configuration n'est requise ou la configuration requise est limitée). Les données collectées par l'Agent de surveillance des temps de réponse sont utilisées pour les tableaux de bord Transactions utilisateur final. Dans , vous pouvez mesurer le temps de réponse du navigateur, et les données de l'Agent de surveillance des temps de réponse sont également utilisées dans la topologie de transaction d'agrégat. Pour plus d'informations, voir «Scénario : Surveillance de la Liste d'applications Java IBM», à la page 98.

Suivi des transactions
Cette fonction est disponible avec Cloud APM, Advanced Private. La fonction de suivi des transactions active les vues de topologie et la surveillance des transactions au niveau de l'instance. Elle est installée en tant qu'élément du serveur Cloud APM. Le suivi des transactions est automatiquement activé pour certains agents mais doit être manuellement activé pour d'autres. Le tableau 3 fournit des informations complémentaires sur les agents qui prennent en charge le suivi des transactions.

Tableau 3. Activation du suivi des transactions pour les agents et les collecteurs de données

Déploiement d'agents ou collecteur de données	Activé par défaut	Méthode d'activation
agent DataPower	✓	«Configuration du suivi des transactions pour l'agent DataPower», à la page 293
agent IBM Integration Bus	—	«Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 333
collecteur de données J2SE	✓	«Configuration de la surveillance de J2SE», à la page 418

Tableau 3. Activation du suivi des transactions pour les agents et les collecteurs de données (suite)

Déploiement d'agents ou collecteur de données	Activé par défaut	Méthode d'activation
agent JBoss	—	«Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 434
collecteur de données Liberty	✓	«Configuration du collecteur de données Liberty pour les applications sur site», à la page 813«Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 845
agent Microsoft .NET	—	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 488
collecteur de données Node.js	—	«Personnalisation du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 556 «Personnalisation du collecteur de données Node.js pour les applications sur site», à la page 563
Agent de surveillance des temps de réponse + agent HTTP Server	—	«Planification de l'installation», à la page 640
Agent SAP NetWeaver Java Stack	—	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 705
Agent Tomcat	—	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 741
Agent WebLogic	—	«Configuration de la surveillance de WebLogic», à la page 750
Agent WebSphere Applications	—	«Configuration du collecteur de données en mode interactif», à la page 774
Agent WebSphere MQ	—	«Configuration du suivi des transactions pour l'Agent WebSphere MQ», à la page 862

Les données sont affichées dans les vues Agréger une topologie de transaction et Topologie des instances de transaction pour tous les agents prenant en charge le suivi des transactions.

Topologie d'application
Voyez comment tous les composants sont connectés dans votre environnement d'application. Pour plus d'informations, voir «Application - Tableau de bord d'Application Performance», à la page 1128.

Topologie des instances de transaction
Visualisez le chemin suivi par chaque instance d'une transaction au sein de votre environnement. Pour plus d'informations, voir «Topologie des instances de transaction», à la page 104.

Synthetic Playback
Vous pouvez surveiller la disponibilité de vos sites Web internes et externes à l'aide de l'Agent Synthetic Playback.

Pour plus d'informations sur l'utilisation des transactions synthétiques, voir «Gestion des transactions et des événements synthétiques», à la page 1058.

Diagnostics approfondis
Pour des agents spécifiques, vous pouvez explorer en aval les tableaux de bord récapitulatifs et les tableaux de bord de diagnostics approfondis de façon à afficher les informations relatives aux demandes individuelles. Explorez en aval les tableaux de bord récapitulatifs pour afficher les détails relatifs aux niveau de code, traces de pile et requêtes SQL. Utilisez les tableaux de bord de diagnostic pour identifier les demandes qui présentent des problèmes et déboguer les transactions problématiques. Vous pouvez également détecter, diagnostiquer ou arrêter les transactions lentes

ou bloquées toujours en cours (voir Agent WebSphere Applications Reference). tableau 4 fournit des informations complémentaires sur les agents de diagnostic.

Tableau 4. Tableaux de bord de diagnostic des agents et collecteurs de données

Agent ou collecteur de données	**Données de diagnostic configurées par défaut**	**Tableaux de bord de diagnostic disponibles**	**Comment accéder aux tableaux de bord de diagnostic**	**Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic**
collecteur de données J2SE	✓	Détail, Modules Web, Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation ou le tableau de bord Modules Web.	«Configuration de la surveillance de J2SE», à la page 418
agent JBoss	–	Tableau de bord de diagnostic, Récapitulatif des demandes en cours, tableau de bord Trace de pile des demandes en cours, Récupération de place par la machine virtuelle Java, Cliché de tas et Comparaison de cliché de tas	Cliquez sur **Diagnostiquer**, **Demandes Inflight**, **Détails** ou **Cliché de tas** dans le tableau de bord Présentation.	«Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 434
collecteur de données Liberty	✓	Détail, Cliché de tas, Comparaison de cliché de tas et Analyse de la mémoire	Cliquez sur **Diagnostiquer**, **Afficher le cliché de tas** ou **Afficher l'analyse de la mémoire** dans le tableau de bord Présentation.	• «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 845 • «Configuration du collecteur de données Liberty pour les applications sur site», à la page 813
agent Microsoft .NET	–	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation.	«Activation de la collecte des données de diagnostic à l'aide de la commande configdc», à la page 489
Agent Node.js	✓	Détails de la récupération de place, Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation.	«Configuration de l'Agent Node.js», à la page 549

Tableau 4. Tableaux de bord de diagnostic des agents et collecteurs de données (suite)

Agent ou collecteur de données	Données de diagnostic configurées par défaut	Tableaux de bord de diagnostic disponibles	Comment accéder aux tableaux de bord de diagnostic	Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic
collecteur de données Node.js	✓	Détails de la récupération de place, Détails des demandes les plus lentes, Instances de demande et Traces des demandes	Cliquez sur **Diagnostiquer** ou **Détails de la récupération de place** dans le tableau de bord Présentation.	• «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 555 • «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 561
collecteur de données Python	✓	Détails des demandes les plus lentes, Détails des traces de demandes, Détails des unités d'exécution Python, Récupération de place Python et Détails des segments de mémoire Python	Cliquez sur **Diagnostiquer**, **Détail des unités d'exécution**, ou **Détails de la mémoire** dans le tableau de bord Présentation.	• «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 624 • «Configuration du collecteur de données Python pour les applications sur site», à la page 629
Agent Ruby	–	Détail récapitulatif des demandes, Exemple d'instances de demande, Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation.	«Configuration de la surveillance de Ruby», à la page 669
collecteur de données Ruby	✓	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation.	«Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 677
Agent SAP NetWeaver Java Stack	✓	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation.	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 705
Agent Tomcat	–	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord Présentation.	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 741

Tableau 4. Tableaux de bord de diagnostic des agents et collecteurs de données (suite)

Agent ou collecteur de données	Données de diagnostic configurées par défaut	Tableaux de bord de diagnostic disponibles	Comment accéder aux tableaux de bord de diagnostic	Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic
Agent WebLogic	—	Tableau de bord de diagnostic, Récapitulatif des demandes en cours, tableau de bord Trace de pile des demandes en cours, JVM GC Detail, Cliché de tas et Comparaison de cliché de tas	Cliquez sur **Diagnostiquer**, **View Requests**, **Détails** ou **Cliché de tas** dans le tableau de bord Présentation.	«Configuration de la surveillance de WebLogic», à la page 750
Agent WebSphere Applications	—	Diagnostics, Instances de demande, Séquence des demandes, Récapitulatif des demandes en cours, Trace de pile des demandes en cours, Cliché de tas, Comparaison de cliché de tas et Analyse de la mémoire	Cliquez sur **Diagnostiquer**, **View Requests**, **View Heap Dump**, ou **View Memory Analysis** dans le tableau de bord Présentation. Le bouton **View Memory Analysis** fonctionne uniquement lorsque la surveillance des fuites de mémoire a été activée.	• «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 771 • «Activation de la surveillance des fuites de mémoire», à la page 810

Le bouton **Diagnostiquer** est activé uniquement si le diagnostic approfondi est configuré pour votre agent et que vous êtes membre du rôle Administrateur de rôles, Administrateur de surveillance, ou de tout autre rôle personnalisé disposant de droits sur la vue des tableaux de bord de diagnostic.

Seuils Les seuils vous permettent de détecter des comportements d'application spécifiques et des conditions en fonction de définitions activement surveillées. Des seuils prédéfinis sont disponibles pour chaque agent et vous pouvez définir de nouveaux seuils pour la surveillance. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1002.

Lorsque la transmission d'événements est configurée, les événements sont envoyés au récepteur EIF. Vous pouvez utiliser le mappage par défaut entre les seuils et les événements transmis au serveur d'événements ou personnaliser la manière dont les seuils sont mappés. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1007.

Dans le **Tableau de bord d'Application Performance**, une fois que vous avez sélectionné une application, l'onglet **Événements** s'affiche. L'onglet **Événements** indique les événements ouverts pour l'application en cours. Vous pouvez accéder à des tableaux de bord détaillés contenant des mesures de performance pour vous aider à déterminer la cause de l'événement. Pour plus d'informations, voir «Statut de l'événement», à la page 1156.

Groupes de ressources

Les systèmes gérés de votre entreprise surveillée peuvent être classés en fonction de leur objet. Ces systèmes gérés possèdent souvent les mêmes exigences de seuil. Utilisez le Gestionnaire de groupes de ressources pour organiser les systèmes surveillés en groupes auxquels vous pouvez affecter des seuils de génération d'événement. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 995.

Page Mise en route

Une fois que vous êtes connecté à la console Cloud APM, la page Mise en route s'affiche. Cliquez sur l'une des **Tâches utilisateur** ou des **Tâches administrateur** pour accéder à une présentation ou une vidéo par scénario. Les liens «Démarrer maintenant» vous permettent d'accéder directement à la fonctionnalité, telle que Gestionnaire de seuils. Les liens **Ressources communautaires** permettent d'accéder à la **Foire aux questions**, au forum Cloud APM et bien plus encore.

Des fonctionnalités supplémentaires sont disponibles par le biais de l'intégration avec d'autres produits et composants. Pour plus d'informations, voir «Intégration» et Chapitre 11, «Intégration à d'autres produits et composants», à la page 871.

Intégration

Des fonctions supplémentaires sont disponibles par le biais de l'intégration à d'autres produits et composants : Tivoli Monitoring, OMEGAMON, Netcool/OMNIbus, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, IBM Cloud, Cloud Private, Tivoli Common Reporting, Alert Notification, Agent Builder et LDAP.

IBM Tivoli Monitoring

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire.Pour plus d'informations, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 872.

Si votre environnement dispose à la fois des produits IBM Tivoli Monitoring et Cloud APM (cloud et/ou sur site), vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management afin d'offrir une vue consolidée des systèmes gérés des deux environnements. Pour plus d'informations, voir «Passerelle hybride», à la page 875. Pour obtenir la liste actuelle des agents Tivoli Monitoring pris en charge, visitez le Hybrid Gateway supported agents (APM Developer Center).

Vous pouvez également configurer des agents Cloud APM pour envoyer des informations d'historique au composant Tivoli Data Warehouse de Tivoli Monitoring afin de les stocker à long terme. Puis, vous pouvez utiliser la version Tivoli Monitoring de Tivoli Common Reporting pour produire les rapports qui incluent des informations d'historique pour ces agents. Pour plus d'informations, voir «Tivoli Data Warehouse pour le rapport de l'historique», à la page 888.

IBM OMEGAMON

Avec OMEGAMON for APM, vous pouvez connecter un ou plusieurs agents OMEGAMON qui s'exécutent sur votre mainframez Systems à Cloud APM. En utilisant OMEGAMON for APM et la Passerelle hybride pour connecter vos agents OMEGAMON déployés dans Cloud APM, vous pouvez visualiser les données de surveillance et les événements associés à vos composants d'application OMEGAMON dans la console Cloud APM.

Pour plus d'informations, voir «Intégration à OMEGAMON», à la page 905.

IBM Netcool/OMNIbus

Vous pouvez réacheminer vos événements de Cloud APM vers votre gestionnaire d'événements Netcool/OMNIbus sur site. Pour plus d'informations, voir «Intégration à Netcool/OMNIbus», à la page 905.

IBM Operations Analytics - Log Analysis

Si votre environnement inclut IBM Operations Analytics - Log Analysis, vous pouvez regrouper les données des journaux d'application et les données de performances pour faciliter la recherche de la cause première des problèmes rencontrés par vos applications. Vous pouvez effectuer des recherches dans les données du journal associées à vos applications pour identifier la cause d'un

problème, comme la lenteur ou un échec. Pour plus d'informations, voir «Intégration à Operations Analytics - Log Analysis», à la page 907.

IBM Operations Analytics - Predictive Insights

Operations Analytics - Predictive Insights analyse les données et apprend le comportement normal d'un système. Il crée un modèle de performance et l'utilise pour détecter ou prévoir le comportement en dehors de la plage modélisée et génère des alarmes en cas de comportement anormal. IBM Cloud Application Performance Management peut être intégré à Operations Analytics - Predictive Insights dans votre environnement. Vous pouvez ensuite afficher les anomalies dans le Tableau de bord d'Application Performance et explorer l'interface utilisateur Operations Analytics - Predictive Insights pour plus de détails. Pour plus d'informations, voir «Intégration à Operations Analytics - Predictive Insights», à la page 908.

IBM IBM Cloud

Vous pouvez afficher les informations de surveillance relatives à vos applications dans l'environnement IBM Cloud à l'aide des collecteurs de données autonomes. Les collecteurs de données permettent l'intégration des fonctionnalités de surveillance à IBM Cloud en transférant les données de surveillance et de diagnostic approfondi des ressources relatives à vos applications IBM Cloud au serveur Cloud APM. Le serveur Cloud APM reçoit et traite les informations de surveillance qui sont collectées par les collecteurs de données. Les types d'applications IBM Cloud suivants peuvent être surveillés :

- Applications Liberty
- Applications Node.js
- Applications Python
- Applications Ruby

Une fois que vous avez configuré un collecteur de données, vous pouvez afficher les données de surveillance sur la console Cloud APM. Pour plus d'informations, voir «Configuration des collecteurs de données», à la page 232.

IBM Cloud Private

Vous pouvez surveiller votre environnement Cloud Private depuis la console Cloud APM. Pour plus d'informations, voir «Surveillance d'IBM Cloud Private», à la page 911.

Tivoli Common Reporting

Intégrez IBM Cloud Application Performance Management à Tivoli Common Reporting pour générer des rapports sur des données fournies par les agents suivants :

- Agent de surveillance des temps de réponse
- Monitoring Agent for Synthetic Playback
- Monitoring Agent for WebSphere Applications

Pour plus d'informations sur l'intégration à Tivoli Common Reporting, voir «Intégration à Tivoli Common Reporting», à la page 917.

Dashboard Application Services Hub

Jazz for Service Management possède une console Concentrateur des services d'application du tableau de bord disposant de fonctionnalités de génération de tableaux de bord personnalisés. Vous pouvez intégrer votre serveur Cloud APM à DASH, puis créer des tableaux de bord dans la console DASH à l'aide des données de vos agents et collecteurs de données Cloud APM. Pour plus d'informations, voir «Intégration à Dashboard Application Services Hub», à la page 925.

IBM Alert Notification

Alert Notification est un système de notification simple et facile d'utilisation qui donne aux informaticiens une notification instantanée des alertes relatives aux problèmes de votre environnement informatique. Les données transmises par les agents fournissent la source des alertes. Une fois que vous avez activé Alert Notification, connectez-le à une instance Cloud APM. En package autonome, vous pouvez intégrer Alert Notification à tout outil de surveillance sur site qui peut implémenter et démarrer une API REST. Les outils pris en charge incluent IBM Tivoli Netcool/OMNIbus. Pour plus d'informations, voir Intégration à Alert Notification.

IBM Agent Builder
Vous pouvez utiliser Agent Builder afin de générer des agents personnalisés pour n'importe quelle technologie. Pour plus d'informations, voir Guide d'utilisation d'IBM Agent Builder.

LDAP Vous pouvez exploiter votre référentiel LDAP dans Cloud APM. Pour obtenir des instructions de configuration, voir «Intégration à LDAP», à la page 931.

Documentation

Vous pouvez trouver des informations sur IBM Cloud Application Performance Management dans l'IBM Knowledge Center, dans la console Cloud APM et dans l'Application Performance Management Developer Center.

IBM Knowledge Center
Cloud APM, Private dans l'IBM Knowledge Center représente la source officiel d'informations techniques pour le produit.

Aide de l'interface utilisateur
Lorsque vous êtes connecté à la console Cloud APM ou explorez la Démonstration guidée, vous pouvez accéder au système d'aide :

- Cliquez sur **Contenu de l'aide** dans la barre de navigation. Menu d'aide.
- Cliquez sur dans la bannière du tableau d'Application Performance.
- Cliquez sur le lien **En savoir plus** dans les pages de configuration système.
- Cliquez sur dans un widget de tableau de bord.

IBM Application Performance Management Developer Center
Application Performance Management Developer Center est un emplacement central pour un grand choix de contenu APM applicable à un large éventail d'utilisateurs d'APM. Le contenu inclut la documentation, les blogues, les vidéos, et les liens vers des ressources additionnelles.

Forum IBM Cloud Application Performance Management et dwAnswers
Le forum Cloud Application Performance Management et dwAnswers contiennent des discussions techniques sur les problèmes relatifs au produit, y compris sur l'identification des incidents et leur résolution.

Des informations sont également disponibles sur les sites Web suivants :

Outil SPCR (Software Product Compatibility Reports)
Vous pouvez utiliser l'outil SPCR pour générer différents types de rapport liés aux offres et aux exigences de composant. Recherchez l'un des noms d'offre Cloud Application Performance Management ou IBM Cloud Application Performance Management - Agents.

IBM Marketplace
Des ressources telles que des démonstrations vidéo et des Foires aux questions sont disponibles dans IBM Marketplace.

IBM Explorateur d'API
Pour obtenir la documentation des API Cloud APM, voir «Exploration des API», à la page 1115.

Terminologie IBM
Le site Web IBM Terminology contient la terminologie relative aux produits IBM accessible depuis dans un emplacement unique.

IBM Redbooks
Les sites Web IBM Redbooks contiennent des publications Redbooks, des Redpapers et des notes techniques de Redbooks qui fournissent des informations sur les produits regroupées par plateformes et solutions.

Conventions utilisées dans la documentation

Plusieurs conventions sont utilisées dans cette documentation pour les termes spéciaux, actions, commandes et chemins en fonction de votre système d'exploitation et pour les informations spécifiques à la plateforme et au produit.

Conventions typographiques

Les conventions typographiques suivantes sont utilisées dans cette documentation :

Gras

- Commandes en minuscules, commandes en casse mixte, paramètres et variables d'environnement difficiles à distinguer du texte qui les entoure
- Contrôles d'interface (cases à cocher, boutons de commande, boutons d'option, toupies, zones, dossiers, icônes, zones de liste, éléments de zones de liste, listes à plusieurs colonnes, conteneurs, choix de menu, noms de menu, onglets, feuilles de propriétés), étiquettes (telles que **Astuce :**)
- Mots clés et paramètres figurant dans le texte

Italique

- Citations (par exemple, titres de publications, de disquettes et de CD)
- Mots et phrases définis dans le texte (exemple : une ligne spécialisée est appelée *ligne point-à-point*)
- Mise en évidence de mots et lettres (exemple : L'adresse du numéro d'unité logique (LUN) doit commencer par la lettre *L*.)
- Nouveaux termes dans le texte, sauf dans la liste des définitions (exemple : une *vue* est un cadre dans un espace de travail contenant des données.)
- Variables et valeurs à fournir (exemple : où *mon_nom* représente...)

`Espace fixe`

- Exemples et exemples de code.
- Noms de fichier, noms de répertoire, chemins, mots clé de programmation, propriétés et autres éléments difficiles à distinguer du texte qui les entoure
- Texte des messages et invites
- Texte que l'utilisateur doit saisir
- Valeurs d'arguments ou d'options de commande

`Espace fixe, gras`

- Noms de commandes et noms de macros et d'utilitaires pouvant être saisis comme des commandes
- Noms de variable d'environnement dans le texte
- Mots clé
- Noms de paramètres dans le texte : paramètres de structure d'API, paramètres et arguments de commande et paramètres de configuration
- Noms de processus
- Noms de variables du registre dans le texte
- Noms de scripts

Variables et chemins d'accès dépendants du système d'exploitation

Le sens de la barre oblique pour les chemins d'accès aux répertoires peut varier dans la documentation. Quel que soit le sens utilisé dans la documentation, observez les recommandations suivantes :

- Linux AIX Utilisez une barre oblique (/).

- Windows Utilisez une barre oblique inversée (\).

Les noms des variables d'environnement ne sont pas toujours identiques sous Windows et AIX. Par exemple, %TEMP% sous Windows correspond à $TMPDIR sous AIX ou Linux.

Pour les variables d'environnement, observez les recommandations suivantes :

- Linux AIX Utilisez **$***variable*.
- Windows Utilisez **%***variable***%**.

Windows Si vous utilisez l'interpréteur de commandes bash sur un système Windows, vous pouvez utiliser les conventions AIX.

Variable et chemins du répertoire d'installation pour le serveur IBM Cloud Application Performance Management

rép_install est le répertoire d'installation du serveur IBM Cloud Application Performance Management. Sur les systèmes d'exploitation Red Hat Enterprise Linux, `/opt/ibm` est l'emplacement par défaut.

Variable et chemins du répertoire d'installation des agents

rép_install correspond au répertoire d'installation des agents. L'emplacement par défaut dépend du système d'exploitation :

- Windows `C:\IBM\APM`
- Linux `/opt/ibm/apm/agent`
- AIX `/opt/ibm/apm/agent`

Chapitre 4. Configuration requise

Divers systèmes d'exploitation sont pris en charge pour les agents et collecteurs de données IBM Cloud Application Performance Management et les exigences varient pour chaque composant. Les exigences du serveur Cloud APM varient en fonction du nombre d'agents que vous souhaitez utiliser pour surveiller les sources de données et du fait que vous utilisiez ou non votre propre serveur Db2.

Autorisations

Vous devez disposez des droits de superutilisateur pour installer et exécuter le serveur Cloud APM. L'exécution du serveur Cloud APM en tant qu'utilisateur non superutilisateur n'est pas prise en charge.

Une fois le serveur Cloud APM installé, vous ne pouvez pas modifier les droits d'accès des fichiers et des répertoires de Cloud APM, ni modifier les propriétaires de groupe ou d'utilisateur de ces fichiers et répertoires.

Fuseau horaire

Utilisez NTP (Network Time Protocol) sur les systèmes gérés et sur le système où est installé le serveur Cloud APM pour garantir l'exactitude de l'heure sur le système. Le réglage de l'heure pour correspondre à l'emplacement physique des serveurs (comme UTC-03:00 pour le Brésil et UTC+06:30 pour Yangon) contribue à assurer un horodatage précis des événements et des transactions.

Exigences des agents et collecteurs de données Cloud APM

Procurez-vous des informations sur les exigences de chaque agent de surveillance et collecteur de données autonome que vous prévoyez d'installer.

L'agent et le collecteur de données Cloud APM sont en général transparents vis-à-vis de l'hyperviseur, ce qui signifie qu'ils peuvent être installés et déployés sur n'importe quel système d'exploitation pris en charge, quels que soient les hyperviseurs sur lesquels les systèmes d'exploitation sont hébergés, tels que Hyper-V, IBM PowerVM, KVM, VMWare ESX, etc.

Pour les exigences des agents et des collecteurs de données, utilisez les liens de la section relative aux rapports sur les composants de la rubrique System requirements (APM Developer Center).

Le système informatique local sur lequel l'agent est installé doit prendre en charge le codage UTF-8 si l'agent envoie des données internationalisées au serveur Cloud APM.

Exigences d'serveur Cloud APM

Pour obtenir les informations les plus récentes sur la configuration requise pour le serveur, notamment en matière de systèmes d'exploitation et leurs versions, de bases de données et de navigateurs Web, utilisez les liens de la section "Product reports" à la page System requirements (APM Developer Center). Par exemple, sélectionnez IBM Cloud Application Performance Management, Advanced V8.1.4. Lorsque le rapport de compatibilité des produits logiciels s'affiche, cliquez sur l'onglet **Prerequisites** pour afficher les exigences de navigateur et de base de données. Cliquez sur l'onglet **Systèmes d'exploitation** afin d'afficher les exigences de système d'exploitation pour le serveur.

Vous pouvez également rechercher le nom de produit dans Software Product Compatibility Reports.

Pour des informations sur les utilisateurs et groupes du serveur Db2 créés par l'installation du serveur Cloud APM, voir la rubrique «Préparation de l'installation du serveur», à la page 125.

© Copyright IBM Corp. 2015, 2018

Eléments prérequis pour serveur Cloud APM

Le serveur Cloud APM et les composants de prise en charge sont installés par un superutilisateur sur un système Red Hat Enterprise Linux.

Pour assurer la réussite de l'installation, consultez les prérequis relatifs au serveur Cloud APM.

Une fois que vous avez lancé l'installation du serveur Cloud APM, un scanner préliminaire se lance automatiquement et vérifie que tous les prérequis sont respectés pour le serveur Cloud APM. Un message d'avertissement ou d'échec s'affiche dans les résultats de l'analyse préliminaire si l'un au moins des prérequis n'est pas respecté. Pour plus d'informations sur l'exécution du scanner de prérequis, voir «Scanner de prérequis», à la page 149

tableau 5 affiche les prérequis pour le serveur Cloud APM et décrit pour chaque prérequis les conditions d'échec et d'avertissement, ainsi que les actions correctives à effectuer.

Tableau 5. Eléments prérequis pour serveur Cloud APM

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
Version du système d'exploitation	La version du système d'exploitation doit être Red Hat Enterprise Linux V6.* ou Red Hat Enterprise Linux V7.*.	La version du système d'exploitation n'est pas prise en charge.	Installez le serveur Cloud APM sur un système d'exploitation pris en charge.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
os.RAMSize	La quantité de mémoire disponible nécessaire dépend de l'offre installée (offre de base ou avancée) et de l'utilisation d'une base de données Db2 locale ou distante. Les exigences en matière de mémoire disponible sont comme suit : • Pour l'offre avancée et une base de données Db2 locale, 24 Go • Pour l'offre avancée et une base de données Db2 distante, 20 Go • Pour l'offre de base et une base de données Db2 locale, 16 Go • Pour l'offre de base et une base de données Db2 distante, 12 Go	Mémoire insuffisante.	Etendez la taille mémoire sur le système au niveau requis.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
Disque	La quantité d'espace disque libre nécessaire dépend de l'offre installée (offre de base ou avancée) et de l'utilisation d'une base de données Db2 locale ou distante. Les exigences en matière d'espace disque libre sont décrites dans la rubrique «Configuration matérielle requise pour le serveur Cloud APM», à la page 92.	Espace disque insuffisant pour effectuer l'installation.	Supprimez les fichiers inutilisés ou agrandissez la partition de disque.
os.swapSize	4 Go ou plus d'espace de permutation libre sont recommandés pour l'installation. Un avertissement s'affiche si la taille d'espace de permutation est comprise entre 2 et 4 Go. L'installation se poursuit mais le serveur risque d'afficher de faibles performances. Une condition FAIL est affichée si la taille de l'espace de permutation est inférieure à 2 Go.	Espace de permutation disponible insuffisant.	Créez ou augmentez l'espace de permutation disponible.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
numLogicalCPU	Le système doit disposer d'au moins 4 UC logiques. Un avertissement s'affiche si le nombre d'UC est compris entre 2 et 4.	Le système doit disposer d'au moins 4 UC logiques.	Augmentez le nombre d'UC logiques.
os.space.homedir	Au moins 1 Go d'espace requis dans le répertoire */home*.	Espace disque insuffisant dans le répertoire */home*.	Supprimez les fichiers inutilisés ou agrandissez la partition de disque.
os.space.installdir	La quantité d'espace libre nécessaire dans le répertoire */rép_install* dépend de l'offre installée (offre de base ou avancée) et de l'utilisation d'une base de données Db2 locale ou distante. Les exigences en matière d'espace libre sont comme suit : • Pour l'offre avancée et une base de données Db2 locale, 80 Go • Pour l'offre avancée et une base de données Db2 distante, 30 Go • Pour l'offre de base et une base de données Db2 locale, 60 Go • Pour l'offre de base et une base de données Db2 distante, 20 Go	Espace disque insuffisant dans le répertoire */rép_install*.	Supprimez les fichiers inutilisés ou agrandissez la partition de disque.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
os.space.tmpdir	Entre 2 et 3 Go d'espace sont requis dans le répertoire temporaire du système pour l'installation.	Espace disque insuffisant dans le répertoire temporaire du système (par exemple, `/tmp/` sous Linux/AIX).	Supprimez les fichiers inutilisés ou agrandissez la partition de disque.
os.dir.opt=dir:/opt/ibm, *type:permission*755+	Le répertoire `/rép_install` doit être accessible au moins en lecture/écriture/exécution pour le propriétaire, et au moins en lecture/exécution pour les groupes et autres.	Une autorisation relative à `rép_install` a été émise.	Vérifiez que le répertoire de partition `rép_install` est accessible au moins en lecture/écriture/exécution pour le propriétaire, et en lecture/exécution pour les groupes et autres. Modifiez les droits relatifs à `rép_install`. Par exemple : `chmod u+rwx,go+rx/rép_install.`
os.umask	La commande umask du shell doit avoir une valeur de 0022.	La commande umask du shell a une valeur différente de 0022. Certains composants, tels que le serveur Db2, ne s'installent pas correctement si les droits d'accès à certains fichiers sont insuffisants.	Affectez à umask la valeur 0022 avant d'exécuter le programme d'installation : `umask 0022; ./install.sh`
os.dir.tmp=dir:/tmp, *type:permission*777+	Le répertoire `/tmp` doit être accessible au moins en lecture/écriture/exécution pour le propriétaire, et au moins en lecture/exécution pour les groupes et autres.	Une autorisation relative au répertoire `/tmp` a été émise.	Vérifiez que le répertoire de partition `/tmp` est accessible au moins en lecture/écriture/exécution pour le propriétaire, et en lecture/exécution pour les groupes et autres. Modifiez les droits sur le répertoire `/tmp`. Par exemple : `chmod u+rwx,go+rx /tmp`
CpuArchitecture	L'unité centrale doit avoir une architecture Intel ou AMD 64 bits.	Le processeur n'a ni une architecture Intel, ni une architecture AMD 64 bits.	Exécutez l'installation du serveur sur un système compatible Intel ou AMD 64 bits.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
rpmdbStatusCorrect	La base de données du package RPM doit être intacte.	La base de données du package RPM n'est pas intacte.	Pour résoudre ce problème, procédez comme suit : 1. Supprimez les fichiers `rm-rf /var/lib/rpm/__db.00* rpm lock`. 2. Pour régénérer la base de données RPM, entrez la commande `rpm --rebuilddb`. 3. Pour désinstaller tous les composants que vous avez installés dans le répertoire `/opt/ibm/`, entrez la commande `/opt/ibm/ccm/uninstall.sh`. 4. Pour redémarrer l'installation, exécutez `./install.sh`.
os.locahostInHostFile	Le nom d'hôte du système hôte local doit être indiqué dans le fichier `/etc/hosts`.	Le nom d'hôte `localhost` n'est pas disponible dans le fichier `/etc/hosts`.	Ajoutez une entrée dans le fichier `/etc/hosts` pour définir le nom d'hôte `localhost`.
os.ulimit= [type:maxprocesseslimit] 4096+	Le système d'exploitation doit permettre à un utilisateur d'avoir au moins 4 097 processus en cours d'exécution. Si la valeur est inférieure, une condition FAIL est renvoyée et l'installation du serveur Cloud APM échoue.	Le nombre maximal de processus utilisateur est trop faible sur ce système d'exploitation.	Pour plus d'informations sur la vérification et la modification des limites, voir «Résolution du nombre maximal d'échecs de processus utilisateur, de fichiers ouverts et de dépendances de fichier ouvert», à la page 84.
os.ulimit= [type:filedescriptorlimit] 32768+	Le système d'exploitation doit permettre à un utilisateur d'avoir au moins 32768 fichiers ouverts. Si la valeur est inférieure, une condition FAIL est renvoyée et l'installation du serveur Cloud APM échoue.	Le nombre maximal de fichiers ouverts est trop faible sur ce système d'exploitation.	Pour plus d'informations sur la vérification et la modification des limites, voir «Résolution du nombre maximal d'échecs de processus utilisateur, de fichiers ouverts et de dépendances de fichier ouvert», à la page 84.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
os.ulimit= [type:corefilesizelimit] 390000+	Le système d'exploitation doit permettre à un utilisateur de créer un cliché du processus core d'au moins 390000 ko. Si la valeur est inférieure, une condition FAIL est renvoyée et l'installation du serveur Cloud APM échoue.	La taille maximale du fichier core est trop faible sur ce système d'exploitation.	Pour plus d'informations sur la vérification et la modification des limites, voir «Résolution du nombre maximal d'échecs de processus utilisateur, de fichiers ouverts et de dépendances de fichier ouvert», à la page 84.
os.mountcheck.tmp_nosuid, s.mountcheck.home_noexec, os.mountcheck.tmp_nosuid, et os.mountcheck.tmp_noexec	Les partitions /tmp ou /home ne doivent pas être montées avec les indicateurs nosuid ou nonexec, ou les deux.	Les partitions `/tmp` ou `/home` sont installées à l'aide des options nosuid ou noexec. L'installation échouera.	Remontez `/tmp` ou `/home` et supprimez les indicateurs nosuid ou noexec.
network.availablePorts.*	Les ports tableau 8, à la page 86 et tableau 9, à la page 88 dans «Ports serveur Cloud APM», à la page 86 doivent être disponibles.	Le port spécifié est indisponible.	Si un pare-feu bloque les ports, vous pouvez le configurer afin d'autoriser le trafic sur certains ports ou le désactiver. Pour plus d'informations, voir «Configuration du pare-feu pour les demandes entrantes sur le serveur», à la page 127.

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
network.ping.Self	Il doit être possible de résoudre le nom d'hôte du système informatique local.	Le nom d'hôte du système informatique local ne peut être résolu.	En cas d'échec du test, effectuez l'une des étapes suivantes : 1. Si vous utilisez un serveur DNS pour la résolution des noms d'hôte, suivez ces étapes : • Vérifiez que le fichier `/etc/resolv.conf` existe et qu'il comporte des entrées pour vos serveurs DNS. • Vérifiez que vos serveurs DNS sont accessibles. Ouvrez une invite de commande et entrez la commande suivante : `ping` *`adresse_IP_serveur_DNS`* 2. Si vous utilisez le fichier `/etc/hosts` pour la résolution des noms d'hôte, vérifiez que le fichier `/etc/hosts` comporte une entrée pour votre système informatique local. 3. Si l'adresse IP de votre système informatique local est affectée par un serveur DHCP, vérifiez que les interfaces réseau sont configurées et qu'une adresse IP et un masque de réseau sont affectés à chaque interface dans la configuration DHCP.
os.package.ksh	Le module KornShell (ksh) requis pour l'agent Summarization and Pruning est manquant.	Le module ksh requis pour l'agent Summarization and Pruning est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.package.bash	Un module bash requis pour le serveur Cloud APM est manquant.	Le module bash requis pour le serveur Cloud APM est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.package.lsof	Le module List Open Files (lsof) requis pour le serveur Cloud APM est manquant.	Le module lsof requis pour le serveur Cloud APM est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
os.package.rsync	Le module rsync requis pour le serveur Cloud APM est manquant.	Le module rsync requis pour le serveur Cloud APM est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.package.unzip	Le module unzip requis pour le serveur Cloud APM est manquant.	Le module unzip requis pour le serveur Cloud APM est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.package.nmap-ncat	Le module nmap-ncat requis pour le serveur Cloud APM est manquant.	Le module nmap-ncat requis pour le serveur Cloud APM est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.package.zip	Le module zip requis pour le serveur Cloud APM est manquant.	Le module zip requis pour le serveur Cloud APM est manquant.	Vous devez installer le module manquant, puis relancer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.lib.libc_64=regex {libc\.so.*}	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.lib.libgcc_64=regex {libgcc.*\.so.*}	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.lib.libstdc_64=regex {libstdc++\.so\.5}	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)

Tableau 5. Eléments prérequis pour serveur Cloud APM (suite)

Prérequis	Description	Description de l'échec dans le rapport d'analyse	Action corrective
os.lib.libstdc_64=regex {libstdc++\.so\.6}	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Une bibliothèque requise pour le serveur Cloud APM est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)

Le tableau 6 affiche les prérequis pour le serveur Cloud APM Db2 et décrit pour chaque prérequis les conditions d'échec et d'avertissement, ainsi que les actions correctives à effectuer.

Tableau 6. Prérequis pour Db2

Prérequis	Description	Description d'incident dans le rapport d'analyse	Action corrective
db2.isInstalled	Un serveur Db2 ne doit pas exister sur le système local.	Une installation existante du serveur Db2 a été détectée sur le système.	Désinstallez le serveur Db2 existant ou choisissez un autre système.
db2.usersNotPresent	Un avertissement s'affiche si des utilisateurs requis par le serveur Db2 sont détectés sur le système. Les utilisateurs sont les suivants : • itmuser • dasusr1 • db2apm • db2fenc1	Des utilisateurs nécessaires au serveur Db2 ont été détectés sur le système.	Supprimez les utilisateurs ou fournissez des mots de passe valides pour les utilisateurs dans le fichier `rép_install/install.properties`, qui est disponible dans le répertoire racine du support d'installation.
db2.groupsNotPresent	Un avertissement s'affiche si des groupes requis par le serveur Db2 sont détectés sur le système.	Des groupes nécessaires au serveur Db2 sont détectés sur le système.	Supprimez les groupes existants ou autorisez le programme d'installation à utiliser les groupes pour l'installation Db2.
db2.servicesNotPresent	Les services Db2 ne doivent pas être en cours d'exécution sur le système.	Des services Db2 en cours d'exécution ont été détectés sur le système.	Désinstallez le serveur Db2 existant, nettoyez tous les services restants ou choisissez une autre système.
os.isUnixServiceRunning .crond	Le serveur Db2 nécessite que le service crond soit en cours d'exécution.	Le service crond n'est pas en cours d'exécution.	Démarrez le service crond. Si vous créez une base de données Db2 sur un système externe ou si vous vous connectez à une base de données MongoDB sur un système externe, vous devez vérifier que le service cron est en cours d'exécution sur ces systèmes.

Tableau 6. Prérequis pour Db2 (suite)

Prérequis	Description	Description d'incident dans le rapport d'analyse	Action corrective
os.kernelversion	L'installation Db2 nécessite le noyau Linux version 2.6.16 ou ultérieure.	La version du noyau n'est pas prise en charge.	Utilisez une version du noyau prise en charge.
os.kernelsNotSupported	Lorsque vous installez l'agent Db2 sur le serveur Db2 et sur certaines machines virtuelles, l'installation nécessite que les versions du noyau Linux ne soient pas comprises entre 2.6.32-434 et 2.6.32-504.7.1	La version du noyau n'est pas prise en charge.	Vous devez effectuer une mise à niveau vers les versions prises en charge. Tout autre noyau à partir de la version 2.6.16 est valide.
os.isLDAPConfigured	Un avertissement s'affiche si LDAP est configuré sur le système.	Le système est configuré pour fonctionner avec LDAP.	Le fichier `/etc/nsswitch.conf` contient des entrées `sss` (System Security Services) ou `ldap` ou `winbind` (Windows Active Directory) pour le mot de passe. Cette situation peut créer des problèmes si des utilisateurs liés à Db2 sont présents dans LDAP et que leur mot de passe est différent de celui défini dans le fichier `rép_install/install.properties`. Si un utilisateur itmuser et des utilisateurs d'instance Db2 sont configurés dans votre annuaire LDAP et que vous envisagez d'installer le serveur Cloud APM avec un serveur Db2 local, suivez les instructions de la rubrique «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.
os.lib.libstdc++_32=regex {libstdc++\.so\.6}	Une bibliothèque requise pour Db2 est manquante.	Une bibliothèque requise pour Db2 est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.lib.pam_64=regex {libpam\.so.*}	Une bibliothèque requise pour Db2 est manquante.	Une bibliothèque requise pour Db2 est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)

Tableau 6. Prérequis pour Db2 (suite)

Prérequis	Description	Description d'incident dans le rapport d'analyse	Action corrective
os.lib.pam_32=regex {libpam\.so.*}	Une bibliothèque requise pour Db2 est manquante.	Une bibliothèque requise pour Db2 est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.package.sg3_utils =sg3_utils	Une bibliothèque requise pour Db2 est manquante.	Une bibliothèque requise pour Db2 est manquante.	Vous devez installer les bibliothèques manquantes, puis relancez l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites» dans «Eléments prérequis pour serveur Cloud APM», à la page 72.)
os.dir.home =[dir:/ home,type:permission] 755+	Le répertoire `/home` des utilisateurs Db2 itmuser, dasusr1, db2apm et db2fenc1 doit être accessible au moins en lecture/écriture/ exécution pour le propriétaire, et au moins en lecture/exécution pour les groupes et autres.	Une autorisation relative au répertoire `/home` a été émise.	Vérifiez si le répertoire `/home` est accessible au moins en lecture/écriture/exécution pour le propriétaire, et en lecture/exécution pour les groupes et autres. Modifiez les droits relatifs à `/home`. Par exemple : `chmod u+rwx,go+rx /home`.

Conseils pour la résolution des dépendances non satisfaites

Pour que l'installation réussisse, vous devez respecter toutes les dépendances du serveur Cloud APM.

Résolution des échecs de dépendance RPM

Le serveur Cloud APM utilise des fichiers RPM (Red Hat Package Manager) pour installer le logiciel. Si les bibliothèques et autres logiciels requis sont manquants, le scanner de prérequis échoue et affiche une explication d'incident, telle que la suivante :

```
Expected                Property                Result      Found
regex(libstdc++.so.6    os.lib.libstdc++_32     FAIL        Unavailable
```

Un client Red Hat Enterprise Linux qui est correctement configuré pour utiliser le gestionnaire de packages yum (Yellowdog Updater, Modified) peut résoudre et installer toute dépendance manquante requise par les fichiers RPM. Pour plus d'informations sur les commandes yum, voir What is yum? How do I use it?.

Lorsque le scanner de prérequis renvoie des erreurs car des dépendances échouent, vous pouvez exécuter la commande `yum provides` *`nom_fonction`*, pour prendre connaissance des éléments requis, et la commande `yum install` *`nom_fonction`* pour installer la dépendance manquante. Par exemple :

Error Le scanner de prérequis affiche le message d'échec suivant :

```
error: Failed dependencies:
libstdc++.so.6 is needed by...
```

Commande «yum provides»

Exécutez la commande suivante :

```
yum provides libstdc++.so.6
```

Le rapport suivant s'affiche :

```
libstdc++-4.4.7-3.el6.i686 : GNU Standard C++ Library
Repo        : installed
Matched from:
Other       : Provides-match: libstdc++.so.6
```

Commande «yum install»

Entrez la commande suivante pour résoudre la fonction manquante :

```
yum install libstdc++-4.4.7-3.el6.i686
```

Commande «yum install»

Entrez la commande suivante pour installer tous les prérequis :

```
yum -y install --setopt=protected_multilib=false ksh libstdc++.i686 pam.i686
pam.x86_64 sg3_utilsbc bc rsync lsof net-tools unzip zip nmap libaio
```

La section tableau 7 affiche quelques messages d'échec qui peuvent survenir lorsque des fichiers et des bibliothèques sont manquants sur Linux, ainsi que le RPM à installer pour les résoudre.

Tableau 7. Exemples de messages d'erreur pour les échecs de dépendances sous Linux et RPM de résolution possibles

Message d'échec	Résolution possible
error: Failed dependencies: libstdc++.so.6 is needed by...	rpm -Uhv libstdc++-4.4.6-4.el6.i686.rpm
error: Failed dependencies: libgcc_s.so.1 is needed by libstdc++-4.4.6-4.el6.i686 libgcc_s.so.1(GCC_3.0) est requis par libstdc++-4.4.6-4.el6.i686 libgcc_s.so.1(GCC_3.3) is needed by libstdc++-4.4.6-4.el6.i686 libgcc_s.so.1(GCC_4.2.0) est requis par libstdc++-4.4.6-4.el6.i686 libgcc_s.so.1(GLIBC_2.0) est requis par libstdc++-4.4.6-4.el6.i686	rpm -Uhv libgcc-4.4.6-4.el6.i686.rpm
error: Failed dependencies: compat-libstdc++-33(i686) is needed by...	rpm -Uhv compat-libstdc++-33-3.2-69.el6.i686.rpm

Résolution du nombre maximal d'échecs de processus utilisateur, de fichiers ouverts et de dépendances de fichier ouvert

Les limites sont définies vis-à-vis du nombre maximal de processus utilisateur, de fichiers ouverts et de taille maximale d'un fichier core sur système où vous souhaitez installer le serveur Cloud APM. Pour connaître les limites, voir «Eléments prérequis pour serveur Cloud APM», à la page 72. Vous pourriez souhaitez contrôler ou modifier ces limites.

Important : Vous devez définir ou modifier les limites de manière permanente plutôt que pour la session shell en cours uniquement en modifiant le fichier `/etc/security/limits.conf`. Les modifications sont ensuite appliquées aux nouvelles sessions et aux nouveaux processus. Vous devez redémarrer le système pour appliquer les modifications. La section ci-dessous présente une configuration conseillée pour le fichier `/etc/security/limits.conf` :

```
* soft nofile 32768
* hard nofile 65536
*  soft  core  unlimited
```

Avertissement : Si vous utilisez les commandes ulimit suivantes pour définir ou modifier les paramètres ulimit, les mises à jour sont temporaires et s'appliquent uniquement à la session utilisateur en cours.

Pour connaître les limites système actuelles, saisissez les commandes suivantes :

- **ulimit -a** renvoie toutes les limites
- **ulimit -u** renvoie le nombre maximal de processus disponibles pour un même utilisateur
- **ulimit -n** renvoie le nombre maximal de descripteurs de fichier ouvert
- **ulimit -c** renvoie la taille maximale du fichier core

Pour augmenter la limite de la session shell en cours, exécutez les commandes suivantes :

- **ulimit -u** *nouvelle_limite* définit le nombre maximal de processus. Par exemple : `ulimit -u 4096`
- **ulimit -n** *nouvelle_limite* définit le nombre maximal de descripteurs de fichier ouvert. Exemple : `ulimit -n 32768`
- **ulimit -c** *nouvelle_limite* définit la taille maximale du fichier core. Exemple : `ulimit -c 390000`

Résolution des dépendances de protocole IPv4 et IPv6 dans l'interface de bouclage

Si `localhost` est défini pour les interfaces IPv4 et IPv6 dans `/etc/hosts`, mais que les protocoles IPv4 et/ou IPv6 sont désactivés dans l'interface de bouclage, le test du scanner des prérequis échoue.

Par exemple, le scanner des prérequis affiche le résultat suivant :

```
Property                              Result   Found                                    Expected
========                            ======    =====    ========
network.loopbackMatchesHosts.ipv6  FAIL      False    True
```

Ce résultat indique que les protocoles dans l'interface de bouclage ne correspondent pas aux valeurs de `localhost` dans le fichier `/etc/hosts`. Pour résoudre ce problème, vous pouvez supprimer la définition `localhost` IPv4/IPv6 dans le fichier hosts ou activer le protocole IPv4/IPv6 dans l'interface de bouclage.

Pour vérifier si les protocoles IPv4 et IPv6 sont définis dans l'interface de bouclage, exécutez **ifconfig** pour cette dernière. Par exemple, si votre interface de bouclage est appelée `lo`, exécutez la commande `ifconfig lo` dans le terminal.

Pour supprimer la définition `localhost` IPv4/IPv6 du fichier hosts, procédez comme suit :

1. Ouvrez le fichier `/etc/hosts` à des fins d'édition.
2. Recherchez les lignes qui contiennent les valeurs définies pour vos interfaces IPv4 et IPv6. Par exemple,

   ```
   127.0.0.1  localhost localhost.localdomain localhost4 localhost4.localdomain4
   ::1  localhost localhost.localdomain localhost6 localhost6.localdomain6
   ```
3. Supprimez le mot `localhost` de la ligne qui contient l'interface IPv4 ou IPv6 qui a entraîné l'échec du scanner de prérequis. Par exemple, remplacez la ligne suivante :

   ```
   ::1  localhost localhost.localdomain localhost6 localhost6.localdomain6
   ```

   par

   ```
   ::1  localhost.localdomain localhost6 localhost6.localdomain6
   ```
4. Sauvegardez le fichier hosts mis à jour et réamorcez votre machine.

Pour activer le protocole IPv4 ou IPv6 dans l'interface de bouclage, exécutez la commande appropriée :

- Pour activer le protocole IPv4, exécutez la commande suivante :

  ```
  sysctl -w net.ipv4.conf.Io.disable_ipv4=0
  ```

  où `Io` est le nom de votre interface de bouclage.
- Pour activer le protocole IPv6, exécutez la commande suivante :

  ```
  sysctl -w net.ipv6.conf.Io.disable_ipv6=0
  ```

  où `Io` est le nom de votre interface de bouclage.

Après avoir activé le protocole, réamorcez votre machine.

Ports serveur Cloud APM

Le scanner de prérequis vérifie si des ports internes et externes sont disponibles pour les communications sur le serveur Cloud APM.

Deux types de port sont utilisés par le serveur Cloud APM :

- Un type de port doit être disponible et ouvert sur le pare-feu. Ces ports sont utilisés pour les communications externes ; vous devez les ouvrir sur le pare-feu ou désactiver le pare-feu. Voir le tableau 8.
- L'autre type de port est utilisé pour les communications internes entre les composants. Ces ports doivent être disponibles mais ils peuvent être bloqués par le pare-feu car ils ne requièrent pas de communications externes. Vous devez empêcher les applications installées sur le serveur Cloud APM de les utiliser. Voir le tableau 9, à la page 88.

Pour chaque port utilisé pour la communication externe, un côté envoie la demande et l'autre côté fournit une réponse. Le côté qui initie la connexion est indiqué pour chaque port dans tableau 8.

Pour obtenir la liste des ports qui doivent être disponibles pour la communication externe sur une Passerelle hybride, voir «Installation de la passerelle hybride», à la page 878.

Le scanner de prérequis vérifie si les ports du tableau 8 et du tableau 9, à la page 88 sont disponibles et renvoie `FAIL` pour chaque port indisponible.

Tableau 8. Ports pour les communications externes

Port	Description
80	Si vous utilisez HTTP pour communiquer avec le serveur Cloud APM, ouvrez le port 80. Les agents et la Passerelle hybride initient une connexion unidirectionnelle avec le serveur Cloud APM sur le port 80. La communication HTTP est l'option par défaut. Le port est libellé sous la forme `MINHTTP` dans la sortie du scanner de prérequis.
443	Si vous utilisez HTTPS pour communiquer avec le serveur Cloud APM, ouvrez le port 443. Les agents et la Passerelle hybride initient une connexion unidirectionnelle avec le serveur Cloud APM sur le port 443. Le port est libellé sous la forme `MINHTTPS` dans la sortie du scanner de prérequis.
8080	Si vous utilisez HTTP pour communiquer avec le serveur Cloud APM, ouvrez le port 8080. Le navigateur console Cloud APM initie une connexion unidirectionnelle avec le serveur Cloud APM sur le port 8080. **Remarque :** Si vous utilisez HTTP et le port 8080 pour vous connecter au serveur Cloud APM, parce que la session de navigateur de la console Cloud APM est redirigée vers HTTPS et le port 9443, activez la communication pour le port 9443. Ce port est libellé sous la forme `APMUIHTTP` dans la sortie du scanner de prérequis.

Tableau 8. Ports pour les communications externes (suite)

Port	Description
9443	Si vous utilisez HTTPS pour communiquer avec le serveur Cloud APM, ouvrez le port 9443. Le navigateur console Cloud APM initie une connexion unidirectionnelle avec le serveur Cloud APM sur le port 9443. Ce port est libellé sous la forme `APMUIHTTPS` dans la sortie du scanner de prérequis.
8099	Ouvrez le port 8099 pour l'authentification OIDC (Open ID Connect). Dans le cadre du processus d'authentification d'utilisateur de la console Cloud APM, il est possible que le navigateur d'un utilisateur soit redirigé vers le port 8099. Le navigateur console Cloud APM initie une connexion unidirectionnelle avec le serveur Cloud APM sur le port 8099. Le port est libellé sous la forme `OIDCHTTPS` dans la sortie du scanner de prérequis.
50000	Si vous configurez le serveur Cloud APM pour la connexion à un serveur Db2 distant, ouvrez le port 50000. Le serveur Db2 ou le serveur Cloud APM peut initier une connexion sur ce port. Ce port est libellé sous la forme `DB2` dans la sortie du scanner de prérequis.
27000	Si vous configurez le serveur Cloud APM pour la connexion à une base de données MongoDB distante, ouvrez le port 27000. Le serveur Cloud APM initie une connexion unidirectionnelle avec MongoDB sur le port 27000. Le port est libellé sous la forme `MONGODB` dans la sortie du scanner de prérequis.
8091 et 8099	Pour utiliser l'API Gestionnaire de seuil ou l'API Resource Group Management Service ou les deux, ouvrez les ports 8091 et 8099. Les utilisateurs de l'API initient une connexion unidirectionnelle avec le serveur Cloud APM. Le port 8091 est libellé sous la forme `SERVER1HTTPS` dans la sortie du scanner de prérequis. Le port 8099 est libellé sous la forme `OIDCHTTPS` dans la sortie du scanner de prérequis.
9443 et 8099	Pour utiliser l'API Contrôle d'accès à base de rôles (RBAC, Role Based Access Control), ouvrez les ports 9443 et 8099. Pour plus d'informations sur l'API RBAC, voir «Accès et utilisation de l'API Role-Based Access Control Service», à la page 1037. Les utilisateurs de l'API initient une connexion unidirectionnelle avec le serveur Cloud APM. Le port 9443 est libellé sous la forme `APMUIHTTPS` dans la sortie du scanner de prérequis. Le port 8099 est libellé sous la forme `OIDCHTTPS` dans la sortie du scanner de prérequis.
9998	Si vous configurez le serveur Cloud APM pour l'envoi des messages EIF à un récepteur EIF, tel que la sonde Probe for Tivoli EIF, ouvrez le port 9998. Si vous souhaitez utiliser un port personnalisé, mettez à jour la valeur du paramètre **Port EIF** dans la catégorie Gestionnaire d'événements de la fenêtre **Configuration avancée** (voir «Gestionnaire d'événements», à la page 1117). Le serveur Cloud APM initie une connexion unidirectionnelle avec le récepteur EIF. Le port est libellé sous la forme `FNEIFRCVR` dans la sortie du scanner de prérequis.
389 ou 636	Si vous envisagez d'authentifier les utilisateurs de la console Cloud APM, ouvrez le port utilisé par votre serveur LDAP. Il s'agit généralement du port 389 mais si vous configurez le serveur LDAP pour requérir des connexions chiffrées SSL/TLS, ouvrez le port 636. Contactez l'équipe chargée des serveurs LDAP pour confirmer les numéros de port utilisés par vos serveurs LDAP. Le serveur Cloud APM initie cette connexion unidirectionnelle avec le serveur LDAP. Ces ports ne sont pas inclus dans la sortie du scanner de prérequis.

Tableau 8. Ports pour les communications externes (suite)

Port	Description
8092 et 8093	Si vous prévoyez d'utiliser la fonction Vue universelle pour définir les tables de tableau de bord dans l'onglet Vues personnalisées du Tableau de bord d'Application Performance, ouvrez les ports 8092 et 8093. Le navigateur console Cloud APM initie une connexion unidirectionnelle avec le serveur Cloud APM sur les ports 8092 et 8093. Les ports sont libellés `UVIEWSHTTP` et `UVIEWSHTTPS` dans la sortie du scanner de prérequis.

Remarque :

- Il est possible d'utiliser d'autres ports pour la communication externe si vous intégrez le serveur Cloud APM à d'autres produits tels que Tivoli Common Reporting. Voir la documentation des produits que vous comptez intégrer au serveur Cloud APM pour déterminer les ports qu'ils utilisent. Pour des liens vers la documentation associée, voir tableau 21, à la page 122 dans la rubrique *Numéros de référence*.
- Si un pare-feu bloque les ports, vous pouvez le configurer afin d'autoriser le trafic sur certains ports ou le désactiver. Pour plus d'informations, voir «Configuration du pare-feu pour les demandes entrantes sur le serveur», à la page 127.

Tableau 9. Ports pour les communications internes entre des composants serveur

Port	Composant
1527	Port de la base de données SCR (Service Component Registry). Le port est libellé sous la forme `SCRDERBYDB` dans la sortie du scanner de prérequis.
2181	Port du processus Zookeeper du courtier de messages Kafka. Ce port est libellé sous la forme `ZOOKEEPER` dans la sortie du scanner de prérequis.
50000	Port du serveur Db2. Si vous vous connectez à un serveur Db2 local, ce port doit être débloqué pour la communication interne. Ce port est libellé sous la forme `DB2` dans la sortie du scanner de prérequis.
6066	Port des applications Spark 2. Le port est libellé sous la forme `SPARKAAPPS2` dans la sortie du scanner de prérequis.
6414	Port pour la base de données Gaian. Le port est libellé sous la forme `FNGAIANDB` dans la sortie du scanner de prérequis.
7077	Port des applications Spark 1. Le port est libellé sous la forme `SPARKAAPPS1` dans la sortie du scanner de prérequis.
18080	Port du maître Spark. Le port est libellé sous la forme `SPARKMASTER` dans la sortie du scanner de prérequis.
18085	Port du travailleur Spark. Le port est libellé sous la forme `SPARKWORKER` dans la sortie du scanner de prérequis.
8090	Port de la connexion d'arrière-plan de la console Cloud APM. Le port est libellé sous la forme `SERVER1HTTP` dans la sortie de scanner de prérequis.
8091	Port de la connexion d'arrière-plan sécurisée de la console Cloud APM. Le port est libellé sous la forme `SERVER1HTTPS` dans la sortie du scanner de prérequis.
9092	Port du courtier de messages Kafka. Le port est libellé sous la forme `KAFKA1` dans la sortie du scanner de prérequis.

Tableau 9. Ports pour les communications internes entre des composants serveur (suite)

Port	Composant
9989	Port du courtier de messages Kafka. Le port est libellé sous la forme `KAFKA2` dans la sortie du scanner de prérequis.
10001	Port du fournisseur de service Open Services for Lifecycle Collaboration. Le port est libellé sous la forme `OSLCPM` dans la sortie du scanner de prérequis.
12315	Port du service d'arrière-plan Java SCR (Service Component Registry). Le port est libellé sous la forme `SCRJAVABKEND` dans la sortie du scanner de prérequis.
27000	Port de la base de données MongoDB. Si vous vous connectez à une base de données MongoDB locale, ce port doit être débloqué pour la communication interne. Le port est libellé sous la forme `MONGODB` dans la sortie du scanner de prérequis.
13245	Port 1 du contrôle d'accès basé sur les rôles. Le port est libellé sous la forme `RBACSERVER1` dans la sortie du scanner de prérequis.
13246	Port 2 du contrôle d'accès basé sur les rôles. Le port est libellé sous la forme `RBACSERVER2` dans la sortie du scanner de prérequis.
13247	Port 3 du contrôle d'accès basé sur les rôles. Le port est libellé sous la forme `RBACSERVER3` dans la sortie du scanner de prérequis.
13248	Port 4 du contrôle d'accès basé sur les rôles. Le port est libellé sous la forme `RBACSERVER4` dans la sortie du scanner de prérequis.
32105	Port de la messagerie interne. Le port est libellé sous la forme `FNINTMSG` dans la sortie du scanner de prérequis.

Ports par défaut utilisés par l'agent et les collecteurs de données

Divers ports sont utilisés pour les communications entre le composant Cloud APM et l'application ou le système (local ou distant) surveillé. Dans la plupart des cas, des ports par défaut sont fournis pour faciliter la configuration. La plupart des valeurs par défaut peuvent être personnalisées à l'aide des paramètres de configuration.

Le tableau 10, à la page 90 répertorie les ports par défaut utilisés par les agents et les collecteurs de données Cloud APM pour communiquer avec les applications ou les systèmes qu'ils surveillent. La mention N/A dans le tableau indique l'un des cas suivants :

- L'agent ou le collecteur de données n'utilise pas de port pour communiquer avec l'application ou le système surveillé.
- Le port utilisé pour les communications est déterminé par la configuration de l'application surveillée.
- Les ports utilisés par l'agent ou le collecteur de données sont affectés de manière dynamique et aucune valeur par défaut statique n'est fournie.
- Tous les ports à utiliser doivent être spécifiés par l'utilisateur et aucune valeur par défaut n'est fournie.

Pour les ports utilisés pour les communications entre le serveur Cloud APM et les agents ou les collecteurs de données, voir «Ports serveur Cloud APM», à la page 86.

Tableau 10. Ports par défaut utilisés par les agents et collecteurs de données

Agents et collecteurs de données	Ports par défaut	Configurable
agent Amazon EC2	N/A	N/A
agent Amazon ELB	N/A	N/A
Agent Azure Compute	• Port TCP 80 (pour HTTP) • Port TCP 443 (pour HTTPS)	Non
agent Cassandra	7199 (pour le serveur JMX)	Oui
agent Cisco UCS	• Port TCP 80 (pour HTTP) • Port TCP 443 (pour HTTPS)	Non
agent Citrix VDI	Pour les appels PowerShell : • 5985 (pour HTTP) • 5986 (pour HTTPS)	Oui
Agent Db2	50000 (port par défaut du serveur Db2)	Oui
agent DataPower	5550 (pour la connexion au dispositif DataPower distant)	Oui
agent Hadoop	• Surveillance locale : valeur de la variable d'environnement **CP_PORT** • Surveillance à distance : – 50070 (Namenode de secours) – 50090 (Namenode secondaire) – 8088 (Gestionnaire de ressources) – 19888 (JobHistory Server) – 8080 (Ambari)	Oui
agent HMC Base	12443 (pour télécharger le SDK à partir de la console HMC)	Non
agent HTTP Server	N/A	N/A
agent IBM Integration Bus	N/A	N/A
Internet Service Monitoring	Pour databridge : • 9510 • 9520	Oui
Agent DataStage	• 9443 (port HTTPS WAS) • 50000 (port JDBC de la base de données)	Oui
collecteur de données J2SE	N/A	N/A
agent JBoss	Varie en fonction de la version du serveur JBoss. • 9990 • 9994 • 9999	Non
collecteur de données Liberty	N/A	N/A
Agent Linux KVM	• 8080 (pour HTTP) • 8443 (pour HTTPS)	Oui
Agent Linux OS	22 (pour la surveillance des journaux à distance avec SSH)	Oui
agent Microsoft Active Directory	N/A	N/A
agent Microsoft Cluster Server	N/A	N/A

Tableau 10. Ports par défaut utilisés par les agents et collecteurs de données (suite)

Agents et collecteurs de données	Ports par défaut	Configurable
agent Microsoft Exchange Server	N/A	N/A
agent Microsoft Hyper-V Server	N/A	N/A
agent Microsoft IIS	N/A	N/A
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	1433 (pour le serveur SQL)	Non
agent Microsoft .NET	5456 (pour le suivi des transactions)	Oui
agent Microsoft Office 365	7799 (pour la transaction synthétique Skype)	Oui
agent Microsoft SharePoint Server	1433 (pour le serveur SQL)	Non
agent Microsoft SQL Server	1433 (valeur par défaut du serveur SQL)	Oui (par **COLL_PORT**)
Agent MQ Appliance	• 162 (pour la réception des événements SNMP) • 5554 (pour la connexion à MQ Appliances)	Oui
Agent MongoDB	• 27017 (pour une instance unique) • 27019 (pour le cluster)	Oui
Agent MySQL	3306 (pour la connexion JDBC)	Oui
agent NetApp Storage	Pour la surveillance à distance : • 8088 • 8488 • 443 • 8443	Non
Agent Node.js	N/A	N/A
collecteur de données Node.js	N/A	N/A
Agent OpenStack	5000 (pour se connecter au service d'identité d'OpenStack)	Oui
Agent Oracle Database	1521 (pour la connexion SQL)	Oui
Agent PHP	N/A	Oui
Agent PostgreSQL	5432 (pour la connexion JDBC)	Oui
collecteur de données Python	N/A	N/A
agent RabbitMQ	15672	Oui
Agent de surveillance des temps de réponse	80 (pour les transactions HTTP)	Oui
Agent Ruby	N/A	N/A
collecteur de données Ruby	N/A	N/A
Agent SAP	33*nn* (*nn* représentant le numéro d'instance SAP)	Non
Agent SAP HANA Database	30013	Oui
Agent SAP NetWeaver Java Stack	50004	Oui
agent Siebel	N/A	N/A
Agent Sterling Connect Direct	1363	Oui
Agent Sterling File Gateway	50000	Oui
Agent Synthetic Playback	4444 (pour se connecter au serveur selenium interne)	Non
Agent Tomcat	8686 (pour le serveur MBean Tomcat)	Oui

Tableau 10. Ports par défaut utilisés par les agents et collecteurs de données (suite)

Agents et collecteurs de données	Ports par défaut	Configurable
Agent UNIX OS	22 (pour la surveillance des journaux à distance avec SSH)	Oui
Agent VMware VI	• 443 (pour la surveillance à distance) • 80 (pour la surveillance locale)	Non
Agent WebLogic	7003	Oui
Agent WebSphere Applications	• 63335 (pour l'agent de surveillance version 8) • 63336 (pour l'agent de surveillance version 6) • 63355 (pour la surveillance des ressources) • 5457 (pour Transaction Framework Extension)	Oui
Agent WebSphere Infrastructure Manager	N/A	N/A
Agent WebSphere MQ	N/A	N/A
agent Windows OS	22 (pour la surveillance des journaux à distance avec SSH)	Oui

Configuration matérielle requise pour le serveur Cloud APM

IBM Cloud Application Performance Management, Private peut être installé sur des systèmes possédant des configurations de disque, de processeur et de mémoire différentes. Le programme d'installation ajuste la configuration de Cloud APM et définit la taille de segment de mémoire Java maximale en fonction de celle du matériel de serveur. La configuration et la taille du serveur peuvent être modifiées après l'installation.

Le serveur Cloud APM doit être installé sur une version prise en charge de Red Hat Enterprise Linux. Pour obtenir une liste des systèmes d'exploitation pris en charge, voir le rapport de compatibilité du produit logiciel relatif à votre offre. Les liens vers ces rapports se trouvent dans le document System requirements (APM Developer Center).

Configuration du serveur requise basée sur la configuration du système

IBM Cloud Application Performance Management gère plusieurs bases de données et peut administrer des milliers de transferts de disque par seconde. Lorsque vous choisissez un système pour exécuter le serveur Cloud APM, sélectionnez un système comportant plusieurs unités de disque dur disponibles (comme le montrent le tableau 11, à la page 93 et le tableau 12, à la page 94), et évitez l'utilisation des unités de disque partagées avec d'autres charges de travail intensives de disque. Dans les environnements virtuels, consultez le propriétaire d'hôte virtuel pour assurer que la capacité d'entrée-sortie adéquate est disponible sur l'hôte.

Les résultats des tests d'échelle indiquent qu'un serveur Cloud APM installé sur un serveur de configuration moyenne ou grande, comme indiqué dans ces tableaux, peut prendre en charge jusqu'à 20 utilisateurs simultanés.

Estimation du nombre de lignes d'agent écrites par minute et de l'espace disque requis pour les bases de données

Pour estimer le nombre de lignes de données d'agent téléchargées par minute , ainsi que l'espace disque requis pour les bases de données Db2 et MongoDB, utilisez la feuille de calcul qui se trouve dans Load projections (APM Developer Center).

Nombre de processeurs

Le nombre de coeurs préconisé vaut pour les unités centrales Entreprise des 1 à 5 dernières

années. Les unités centrales plus anciennes nécessitent des coeurs supplémentaires pour obtenir les mêmes performances. Vous pouvez consulter le site Web des SPEC (Standard Performance Evaluation Corporation) à l'adresse http://www.spec.org, et y rechercher un processeur ayant une valeur SPECint2006 supérieure à 30. L'augmentation du nombre et de la vitesse des coeurs de processeur améliore les performances et réduit le temps nécessaire à l'arrêt et au redémarrage des composants serveur.

Mémoire
La quantité suggérée de mémoire (RAM) pour le système qui exécute le serveur Cloud APM (en gigaoctets). Les systèmes dotés de moins de mémoire peuvent voir leurs performances diminuer en raison d'un cache de fichiers moins large et d'une permutation accrue.

Il est recommandé d'avoir au moins 4 Go d'espace de permutation pour l'installation des composants serveur Cloud APM.

Espace disque
Il s'agit d'une estimation de la quantité d'espace disque requise pour une installation moyenne de cette taille d'environnement surveillée. Les utilisations de l'espace disque peuvent varier en fonction du nombre et des types d'agent installés, ainsi que du nombre de transactions surveillées (ne faisant pas partie de l'environnement Cloud APM, Base Private). Pour une estimation plus détaillée de l'utilisation du disque dans votre environnement, utilisez la feuille de calcul qui se trouve dans Load projections (APM Developer Center).

Au moins 3 Go d'espace est requis dans le répertoire temporaire du système pour l'installation des composants du serveur Cloud APM.

Nombre d'unités de disque dur
Le nombre d'unités de disque dur est le nombre total d'unités sur lesquelles se répartit la charge de travail dans une grappe segmentée ou R7AID 0 (pour des performances d'entrée-sortie améliorées). Pour la protection des données, il est préférable d'utiliser RAID 10, qui double le nombre des unités de disque dur requises. RAID 5 n'est pas recommandé pour le serveur Db2 en raison de sa faible performance en écriture. Il est préférable d'utiliser un contrôleur RAID ou une mise en cache de disque dur (avec batterie de secours) pour obtenir le temps d'attente de disque essentiel aux opérations de base de données. Le nombre d'unités peut être ajusté d'après la vitesse et le temps d'attente de vos contrôleurs et unités système d'entrée-sortie.

Transactions par seconde d'entrée-sortie de disque
Transactions par seconde d'entrée-sortie de disque est le nombre moyen de transactions de disque (lectures ou écritures) par seconde que le serveur Cloud APM génère sur le sous-système d'E-S (disques) pour cette taille d'environnement surveillé.

Transactions utilisateur surveillées par seconde
Lorsqu'un utilisateur interagit avec une application, telle une page Web, plusieurs composants surveillés peuvent intervenir dans chaque transaction. Une application peut présenter divers niveaux de complexité. Les estimations qui suivent supposent que 5 à 7 composants surveillés interviennent dans une transaction utilisateur moyenne.

serveur Db2 distant
Pour plus d'informations sur l'utilisation d'un serveur Db2 externe dans la configuration du serveur Cloud APM, voir «Connexion à un serveur Db2 distant», à la page 129.

Tableau 11. IBM Cloud Application Performance Management, Base Private : configuration matérielle requise du serveur basée sur la configuration du système

Offre IBM Cloud Application Performance Management, Base Private		**Classification des tailles d'environnement Cloud APM**		
		Petite	**Moyenne**	**Grande**
Attributs d'environnement surveillé	Nombre de systèmes gérés	Moins de 400	400 à 2000	2000 à 10000
	Lignes d'agent écrites par minute	Moins de 20 000	20 000 à 150 000	150 000 à 500 000

Tableau 11. IBM Cloud Application Performance Management, Base Private : configuration matérielle requise du serveur basée sur la configuration du système (suite)

Offre IBM Cloud Application Performance Management, Base Private		**Classification des tailles d'environnement Cloud APM**		
		Petite	**Moyenne**	**Grande**
Un seul serveur - tous les composants sont sur le même système	Nombre de processeurs	4	6	8
	Mémoire (Go)	16	20	28
	Espace disque (Go)	60	60 à 500	500 à 2000
	Nombre d'unités de disque dur	1	2 à 3	5 à 6
	Transactions par seconde d'entrée-sortie de disque	200	200 à 500	500 à 3000
serveur Cloud APM avec Db2 installé sur le système distant	Nombre de processeurs	4	6	8
	Mémoire (Go)	12	16	20
	Espace disque (Go)	20	20 - 50	50 - 100
	Nombre d'unités de disque dur	1	1	2
	Transactions par seconde d'entrée-sortie de disque	100	100 à 200	200 à 500
serveur Db2 distant	Nombre de processeurs	2	2	4
	Mémoire (Go)	2	4	8
	Espace disque (Go)	40	40 à 500	500 à 2000
	Nombre d'unités de disque dur	1	2	4
	Transactions par seconde d'entrée-sortie de disque	100	100 à 400	400 à 2500

Remarque : Un système géré est un système d'exploitation, un sous-système ou une application unique de votre entreprise surveillé par un agent.

Tableau 12. IBM Cloud Application Performance Management, Advanced Private : configuration matérielle requise du serveur basée sur la configuration du système

Offre IBM Cloud Application Performance Management, Advanced Private		**Classification des tailles d'environnement Cloud APM**		
		Petite	**Moyenne**	**Grande**
Attributs d'environnement surveillé	Nombre de systèmes gérés	Moins de 400	400 à 2000	2000 à 10000
	Lignes d'agent écrites par minute	Moins de 20 000	20 000 à 150 000	150 000 à 500 000
	Transactions utilisateur surveillées par seconde	Moins de 50	50 - 150	150 à 600
Un seul serveur - tous les composants sont sur le même système	Nombre de processeurs	6	8	16
	Mémoire (Go)	24	32	40
	Espace disque (Go)	80	80 à 1000	1000 à 3000
	Nombre d'unités de disque dur	1	3 à 4	6 à 8
	Transactions par seconde d'entrée-sortie de disque	500	500 à 1500	1500 à 4500

Tableau 12. IBM Cloud Application Performance Management, Advanced Private : configuration matérielle requise du serveur basée sur la configuration du système (suite)

Offre IBM Cloud Application Performance Management, Advanced Private		**Classification des tailles d'environnement Cloud APM**		
		Petite	**Moyenne**	**Grande**
serveur Cloud APM avec Db2 installé sur le système distant	Nombre de processeurs	6	8	12
	Mémoire (Go)	20	24	28
	Espace disque (Go)	30	30 à 100	100 à 400
	Nombre d'unités de disque dur	1	2	3
	Transactions par seconde d'entrée-sortie de disque	200	200 à 500	500 à 1500
serveur Db2 distant	Nombre de processeurs	2	2	4
	Mémoire (Go)	2	8	16
	Espace disque (Go)	50	50 - 1000	1000 à 3000
	Nombre d'unités de disque dur	1	2 à 3	4 à 6
	Transactions par seconde d'entrée-sortie de disque	300	300 à 1000	1000 à 3000

Taille de segment de mémoire Java

Suivant la manière dont le programme d'installation classe le système, la taille de segment de mémoire Java maximale est définie pour les services Cloud APM avec les valeurs indiquées dans tableau 13. Si vous mettez à jour l'environnement après l'installation en ajoutant de la mémoire ou des processeurs de sorte que vous passez dans une autre classe de taille (par exemple, de petite à moyenne), exécutez le script **`server_size.sh`** pour reconfigurer les paramètres de taille de segment de mémoire Java maximale. Pour plus d'informations, voir «Gestion de la taille du segment de mémoire Java maximale et du pool de mémoire tampon Db2», à la page 1093.

Tableau 13. Paramètre de taille de segment de mémoire Java

serveur Cloud APM, composants	**Petite**	**Moyenne**	**Grande**
Serveur d'applications server1	1536 Mo	2048 Mo	3072 Mo
Service APMUI	1536 Mo	3072 Mo	4096 Mo
Uviews (instance de serveur Liberty)	1024 Mo	1024 Mo	1024 Mo
MIN (instance de serveur Liberty)	512 Mo	1536 Mo	2048 Mo
OIDC	128 Mo	128 Mo	256 Mo
Kafka	256 Mo	512 Mo	512 Mo
Zookeeper	256 Mo	256 Mo	256 Mo
MongoDB Cache	1024 Mo	2048 Mo	4096 Mo

Remarque : La taille de segment de mémoire cache de MongoDB est de 1024 Mo pour toutes les installations de Cloud APM, Base Private.

Agents de surveillance IBM

Utilisez ces informations pour télécharger les documents pour les agents de surveillance IBM.

Informations sur l'installation et la configuration

Consultez le *Guide d'installation et de configuration* de l'agent pour obtenir les informations spécifiques suivantes :

- Exigences
- Contrôle des conditions préalables
- Installation des modules de langue
- Installation et configuration propres à l'agent

Informations de référence

Voir Informations de référence pour obtenir les informations propres à l'agent suivantes :

- Groupes d'attributs et attributs
- Espaces de travail
- Situations
- Commandes Action
- Stratégies
- Mappage d'événements

Informations sur la résolution des problèmes

Consultez le *Guide d'identification des incidents* pour obtenir les informations propres à l'agent suivantes :

- Consignation de trace
- Incidents et solutions
- Informations de support
- Présentation des messages d'information, d'avertissement et d'erreur

Téléchargez les documents liés à un agent de surveillance donné à partir des liens disponibles dans le tableau suivant :

Tableau 14. Liens de document

Agent de surveillance	Guide d'installation et de configuration	Référence d'agent	Guide d'identification des incidents
IBM Monitoring Agent for SAP HANA Database V7.1.1	IBM Tivoli Monitoring Agent for SAP HANA Database Installation and Configuration Guide	IBM Tivoli Monitoring Agent for SAP HANA Database Reference Guide	IBM Tivoli Monitoring Agent for SAP HANA Database Troubleshooting Guide
IBM Monitoring Agent for Hadoop V7.10.0.0	IBM Tivoli Monitoring Agent for Hadoop Installation and Configuration Guide	IBM Tivoli Monitoring Agent for Hadoop Reference Guide	IBM Tivoli Monitoring Agent for Hadoop Troubleshooting Guide

Chapitre 5. Scénarios

Selon la complexité de votre environnement, vous devez installer différents agents pour surveiller différents composants. Appuyez-vous sur ces scénarios de déploiement pour comprendre quels éléments vous devez installer et où les installer afin d'obtenir les meilleurs résultats d'IBM Cloud Application Performance Management.

Scénario : Surveillance d'IBM API Connect

Vous pouvez surveiller votre environnement IBM API Connect, mais également en identifier et résoudre les problèmes, à l'aide des agents et collecteurs de données APM.

Le produit Cloud APM vous aide à gérer les performances et la disponibilité de votre environnement API Connect. A l'aide des agents et collecteurs de données Cloud APM, vous disposez d'une visibilité et d'un contrôle sur l'infrastructure API Connect et les API d'application, pour garantir des performances optimales et une utilisation efficace des ressources. Si vous rencontrez des problèmes de performance dans l'environnement API Connect, le produit Cloud APM peut vous aider à les détecter, diagnostiquer et isoler.

Par exemple, vous pouvez installer les agents de système d'exploitation sur tous les systèmes applicables. Ces agents permettent de collecter et d'analyser les performances du serveur, y compris les performances de l'UC, les E-S de disque et l'utilisation, la disponibilité et les performances des processus et les performances du réseau. Ils peuvent, de plus, être configurés pour surveiller les journaux clés et les journaux système d'API Connect.

De plus, vous pouvez déployer l'Agent Synthetic Playback et créer des transactions synthétiques et des événements pour surveiller la disponibilité et les performances de vos applications internes et externes. Pour plus d'informations sur cet agent, voir Surveillance de Synthetic Playback.

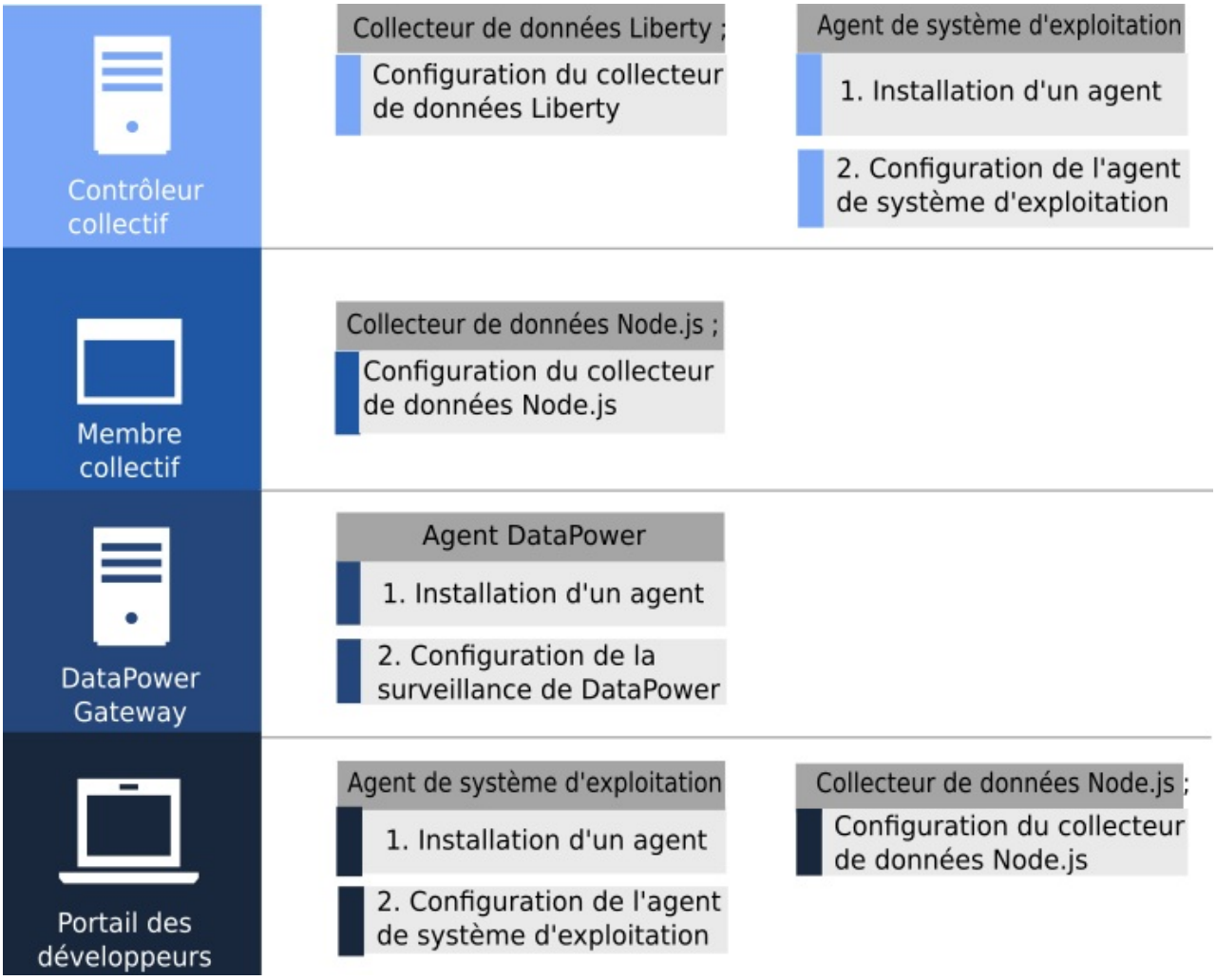
Si d'autres produits middleware sont déployés, la fonction de suivi des transactions, installée comme faisant partie du serveur Cloud APM, fournit des vues de topologie permettant d'afficher les informations de suivi des transactions pour les produits middleware et les services qu'ils proposent et pour traiter les problèmes le cas échéant.

L'image ci-après illustre les composants API Connect et les agents et collecteurs de données Cloud APM correspondants qui peuvent les surveiller. Pour activer ces agents et collecteurs de données, effectuez les tâches d'installation et de configuration répertoriées sous le nom de l'agent et du collecteur de données. Cliquez sur les cases rectangulaires de l'image qui contient le nom de tâche pour accéder aux tâches d'installation ou de configuration.

Remarque :

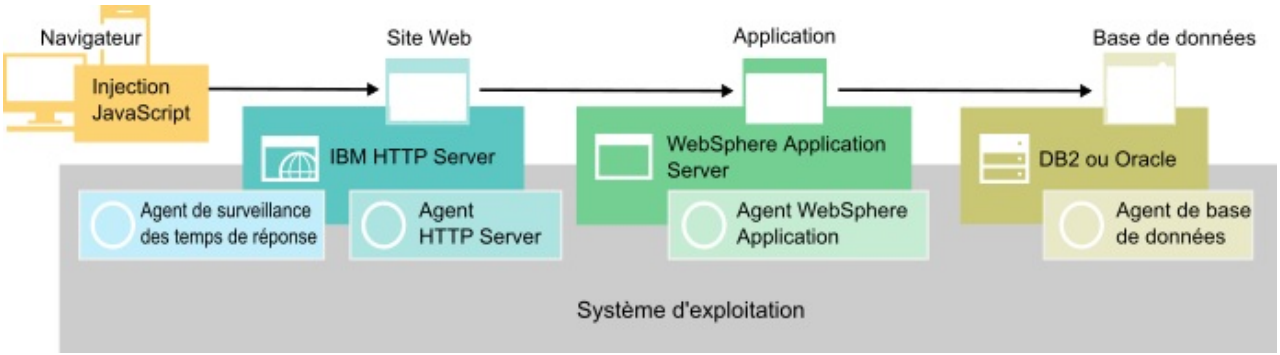
- Installez un collecteur de données Node.js sur chaque application IBM API Connect publiée dans le membre de collectivité.
- Lors de la surveillance de DataPower Gateway, l'agent DataPower s'exécute à distance à partir du dispositif DataPower.

© Copyright IBM Corp. 2015, 2018



Scénario : Surveillance de la Liste d'applications Java IBM

Vous pouvez surveiller et traiter les incidents relatifs à la Liste d'applications Java IBM pour afficher des informations de surveillance des transactions transmises à partir du navigateur vers la base de données, y compris des informations de surveillance des ressources à partir des composants individuels. La Liste d'applications Java IBM inclut IBM HTTP Server, WebSphere Application Server et la base de données IBM Db2 ou Oracle.



Surveillance de la Liste d'applications Java IBM

Pour surveiller la Liste d'applications Java IBM, installez les agents répertoriés pour chaque composant dans l'ordre indiqué.

(Facultatif) Si vous souhaitez également surveiller le système, installez les agents de système d'exploitation sur tous les composants.

Pour le serveur Web, procédez comme suit :

1. Installez l'agent HTTP Server.

   Raccourci : Cette installation comprend l'installation du module IBM HTTP Server Response Time et configure automatiquement l'injection de JavaScript.
2. Configurez l'installation de l'agent HTTP Server..
3. Installez l'agent Response Time Monitoring.

Pour le serveur d'applications, installez l'Agent WebSphere Applications.

Pour la base de données, installez l'agent Oracle Database ou l'agent Db2, selon votre base de données.

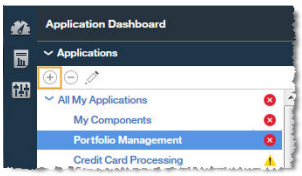
Ajout d'applications Web au Tableau de bord d'Application Performance

Ajoutez les applications à surveiller au Tableau de bord d'Application Performance.

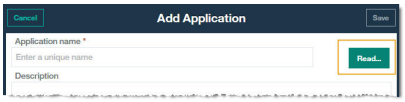
Procédure

Pour ajouter des applications Web, procédez comme suit :

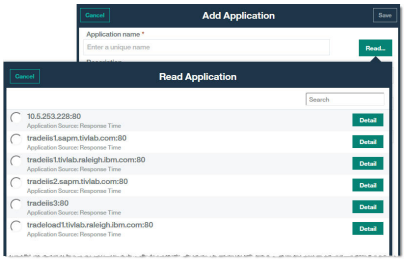
1. Dans le Tableau de bord d'Application Performance, cliquez sur **Ajouter une application**.



2. Cliquez sur **Lire** pour ouvrir la liste des applications reconnues.



3. Sélectionnez l'application Web à surveiller.



4. Cliquez sur **Sauvegarder**.

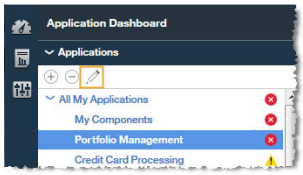
Association d'une Liste d'applications Java IBM à l'application Web

Editez l'application Web pour associer les composants WebSphere Application Server et de base de données à inclure dans la surveillance.

Procédure

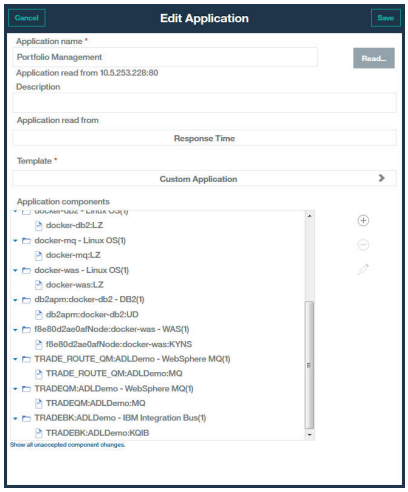
Pour afficher les composants de la Liste d'applications Java, procédez comme suit dans le Tableau de bord d'Application Performance :

1. Sélectionnez le serveur Web et cliquez sur **Modifier une application**.



2. Dans la fenêtre Modification d'application, cliquez sur **Ajouter des composants** + .
3. Dans la fenêtre Sélectionner le composant, sélectionnez WebSphere Application Server.
4. Dans l'Editeur de composants, sélectionnez les instances de composant requises et cliquez sur **Ajouter**.

   Toutes les instances WebSphere Application Server détectées sont ajoutées automatiquement à cette liste.
5. Cliquez sur **Précédent** et répétez les étapes 3 - 4 pour votre base de données. Ajoutez les autres instances de WebSphere Application Server et de base de données nécessaires à la Liste d'applications Java.



6. Cliquez sur **Fermer**, puis sur **Sauvegarder** pour revenir au Tableau de bord d'Application Performance.

Résultats

Conseil : Si le tableau de bord Agréger une topologie de transaction ne contient pas la topologie attendue, attendez que celui-ci s'actualise, puis vérifiez de nouveau quelques minutes plus tard. Si la topologie ne répond toujours pas à vos attentes, il est possible que votre application ne communique pas avec les composants prévus. Vérifiez votre environnement.

Affichage des résultats de la surveillance de la Liste d'applications Java IBM

Vous pouvez afficher les résultats de la surveillance de la Liste d'applications Java IBM dans les topologies.

Pourquoi et quand exécuter cette tâche

Les topologies contiennent des informations de surveillance des transactions transmises à partir du navigateur vers la base de données, y compris des informations de surveillance des ressources à partir des composants individuels. Les tableaux de bord Agréger une topologie de transaction et Topologie des instances de transaction contiennent les noeuds suivants :

- Navigateur, affiché uniquement lorsque l'injection de JavaScript est activée
- Serveur HTTP
- WebSphere Application Server
- Base de données

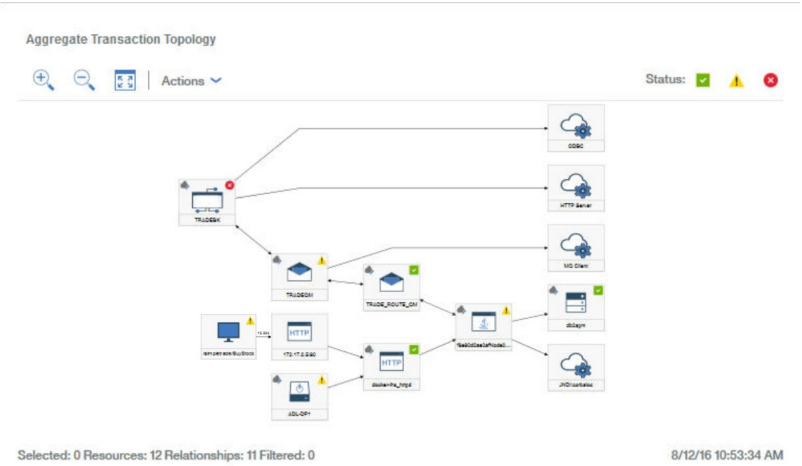
Procédure

Vous pouvez créer un lien entre les noeuds de la topologie et les détails supplémentaires sur ce noeud :

1. Survolez un noeud à l'aide de votre souris pour afficher une fenêtre contenant des informations supplémentaires.
2. Pour explorer un tableau de bord plus détaillé pour le noeud, cliquez avec le bouton droit de la souris sur le noeud et sélectionnez le lien.

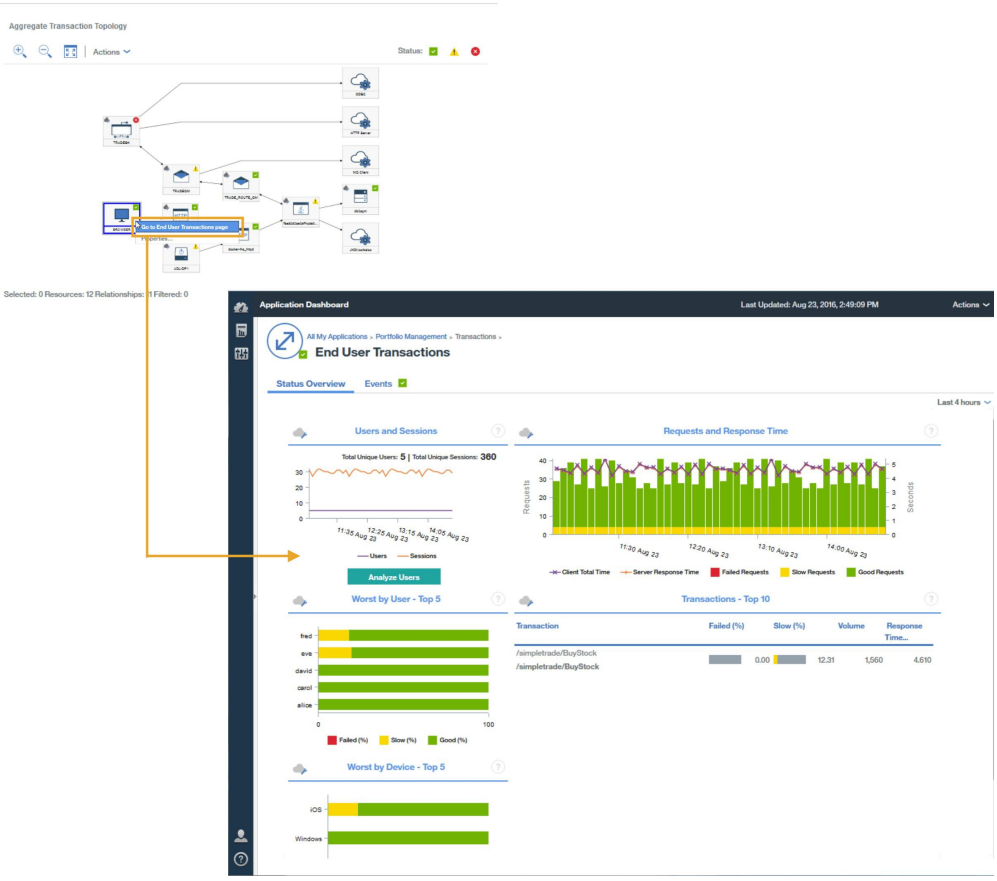
Agréger une topologie de transaction

Le widget Agréger une topologie de transaction est affiché dans le tableau de bord Récapitulatif de l'application.



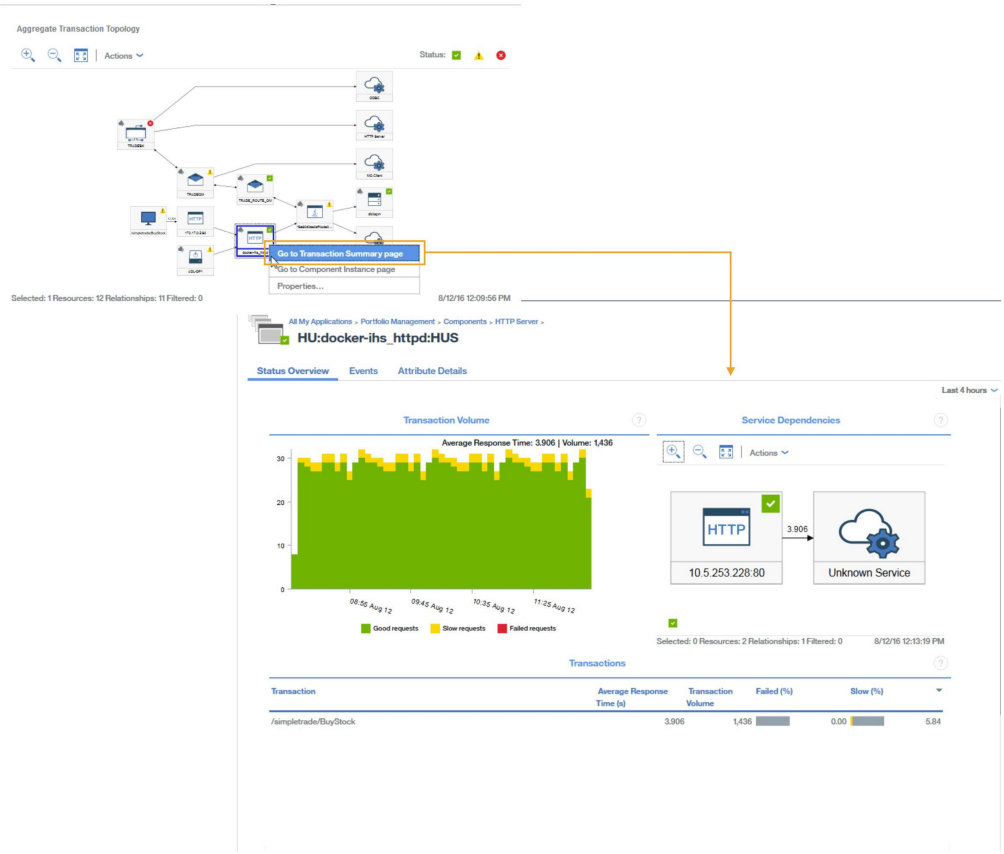
Le widget Agréger une topologie de transaction affiche les informations suivantes :

- Noeud pour les clients exécutables dans un navigateur, exploration détaillée de l'expérience d'utilisateur final



A faire : Ce noeud est affiché uniquement lorsque l'injection automatique de JavaScript mesure les données collectées par le navigateur.

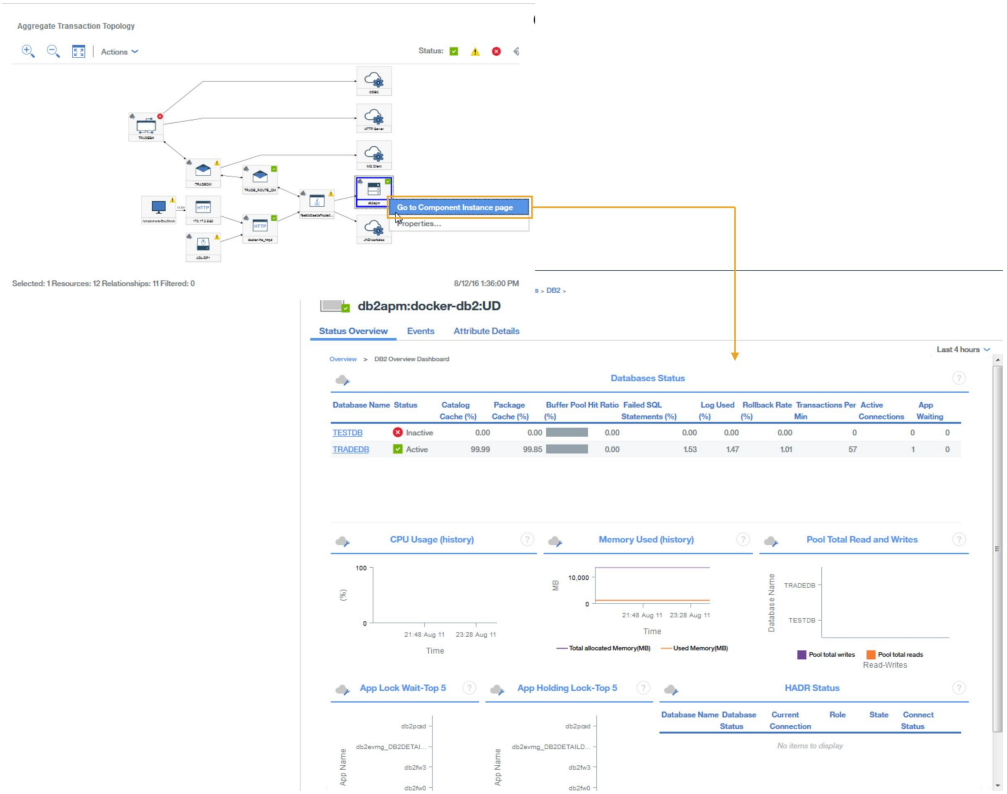
- Noeuds pour les applications HTTP, exploration détaillée de la page des ressources du serveur Web ou de la page de récapitulatif des transactions



- Noeuds pour les applications basées sur WebSphere Application Server, exploration détaillée d'une page des ressources d'applications ou d'une page de récapitulatif des transactions



- Noeuds pour des serveurs de bases de données spécifiques, exploration détaillée de la page des ressources de base de données si disponible

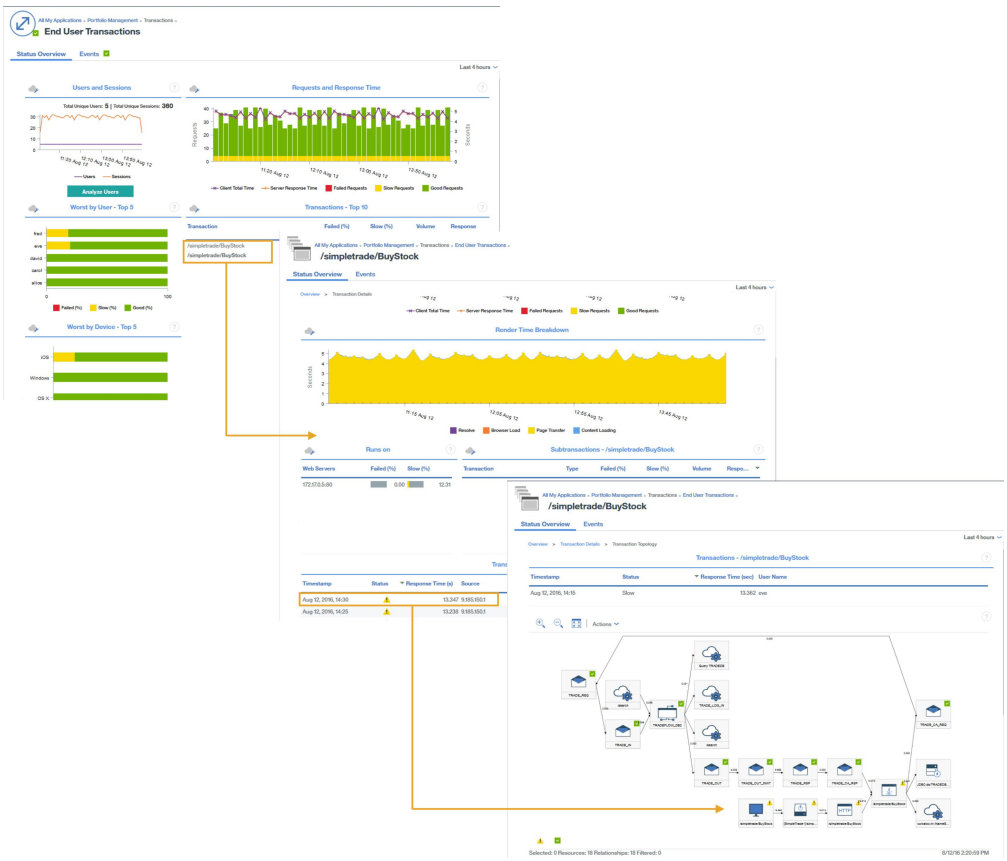


Topologie des instances de transaction

Les topologies des instances de transaction sont affichées pour les transactions d'utilisateur final réelles.

Accédez aux widgets suivants à partir du récapitulatif Transactions utilisateur final :

1. Sélectionner une transaction dans le tableau Transactions - 10 premières.
2. Sélectionner une instance dans le tableau Instances de transaction



Les topologies des instances de transaction pour la pile d'application Java affichent les noeuds suivants. Cliquez sur un noeud pour accéder à ses informations.

- Noeud pour les clients exécutables dans un navigateur

  A faire : Ce noeud est affiché uniquement lorsque l'injection automatique de JavaScript mesure les données collectées par le navigateur.
- Noeuds HTTP, y compris les temps de réponse du navigateur
- Noeuds DataPower, s'ils sont instrumentés
- Noeuds WebSphere Application Server incluant le détail d'une page des ressources d'application
- Noeuds de serveurs de base de données incluant le détail du statut d'une ressource de base de données et des informations de diagnostic d'instruction SQL pour les demandes JDBC

  Conseil : Lorsque la topologie indique que la plus grande partie du temps de réponse est utilisée dans la base de données, les informations d'instruction SQL sont directement ouvertes si vous cliquez sur **Diagnostiquer**.

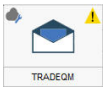
Les diagrammes de Gantt, qui récapitulent les temps des instances, sont également affichés.

Diagnostic des incidents de votre environnement

Si les instances de transaction de l'un des composants de votre environnement sont lentes ou en échec alors le statut approprié est affecté au composant impacté.

Un noeud peut avoir l'un des statuts suivants :

- 

Satisfaisant : le noeud est caractérisé par une coche entourée d'un carré vert qui s'affiche dans l'angle supérieur droit
- 

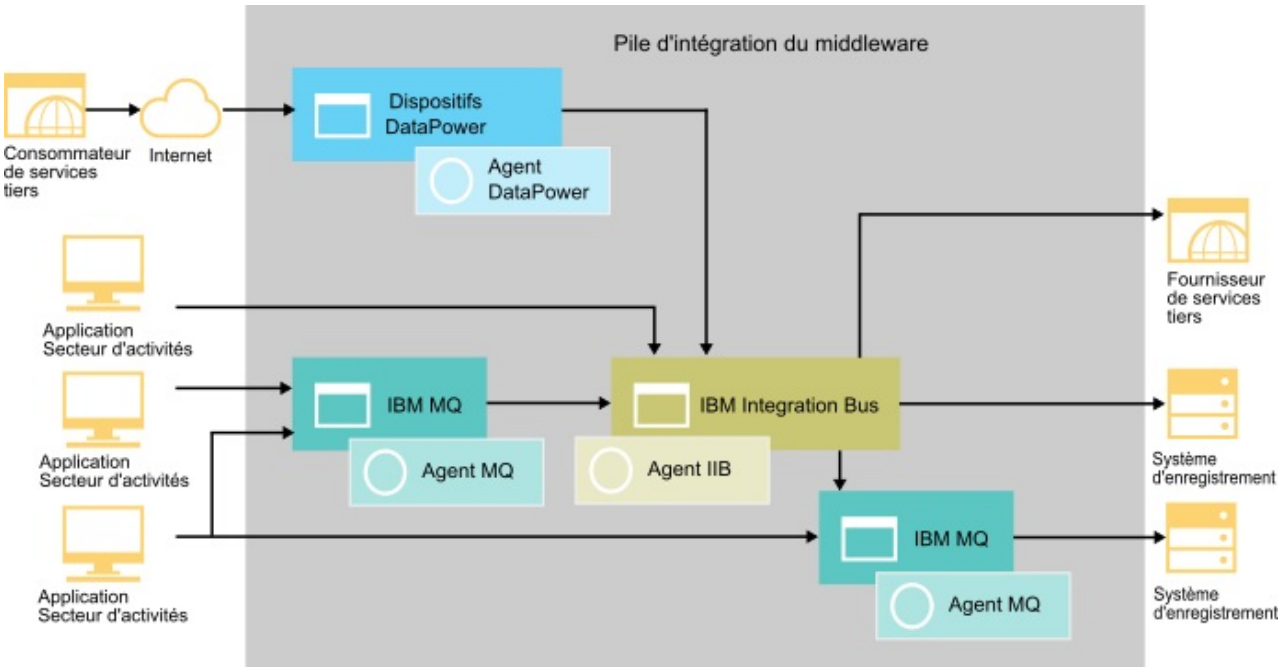
Avertissement : le noeud est caractérisé par un point d'exclamation entouré d'un triangle jaune qui s'affiche dans l'angle supérieur droit
- 

Critique : l'arrière-plan du noeud est rouge et une croix dans un cercle rouge s'affiche dans l'angle supérieur droit

Pour identifier la nature des problèmes liés aux composants dont le statut est avertissement ou critique, cliquez avec le bouton droit de la souris sur le noeud et examinez en détail les informations sur les causes probables des incidents.

Scénario : Surveillance de la Pile d'intégration IBM

Vous pouvez surveiller la Pile d'intégration IBM afin d'afficher des informations de suivi des transactions pour les produits middleware et les services qu'ils proposent et pour traiter les problèmes le cas échéant. La Pile d'intégration IBM contient IBM MQ, IBM Integration Bus et dispositif DataPower.



Surveillance de la Pile d'intégration IBM

Pour surveiller la Pile d'intégration IBM, installez les agents répertoriés pour chaque composant dans l'ordre indiqué.

(Facultatif) Si vous voulez également surveiller un système, installez les agents de système d'exploitation sur ce système.

Pour IBM MQ, procédez comme suit :

1. Installez l'agent de surveillance pour WebSphere MQ.

2. Configurez l'Agent WebSphere MQ pour la connexion au gestionnaire de files d'attente.
3. Activez **Trace de l'activité de l'application MQ** dans le gestionnaire de files d'attente.

Pour IBM Integration Bus, procédez comme suit :
1. Installez l'agent de surveillance pour IBM Integration Bus.
2. Activez IBM Integration Bus pour le suivi des transactions.
3. Configurez le suivi des transactions pour les instances de l'agent IBM Integration Bus requises.

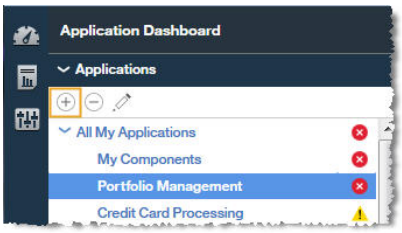
Pour dispositif DataPower, procédez comme suit :
1. Installez l'agent de surveillance pour DataPower.
2. Configurez l'agent DataPower pour vous connecter au dispositif DataPower.
3. Vérifiez que le suivi des transactions est activé pour les instances de l'agent DataPower requises.
4. Configurez le dispositif DataPower.

Ajout d'applications middleware au Tableau de bord d'Application Performance

Créez une application Pile d'intégration IBM et ajoutez-y les instances IBM MQ, IBM Integration Bus et dispositif DataPower que vous souhaitez surveiller.

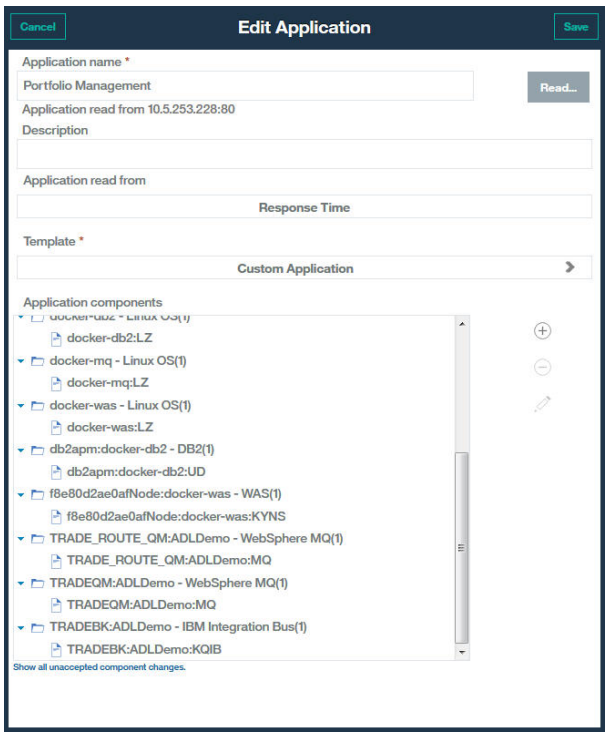
Procédure

Pour afficher les composants de la Pile d'intégration IBM, procédez comme suit dans le Tableau de bord d'Application Performance :
1. Dans le Tableau de bord d'Application Performance, cliquez sur **Ajouter une application**.



2. Dans la fenêtre Modification d'application, ajoutez un nom d'application, puis cliquez sur **Ajouter des composants** +.
3. Dans la fenêtre Sélectionner le composant, sélectionnez **IBM Integration Bus**.
4. Dans l'Editeur de composants, sélectionnez les instances de composant requises et cliquez sur **Ajouter**.

   Toutes les instances IBM Integration Bus détectées sont ajoutées automatiquement à cette liste.
5. Cliquez sur **Précédent** et répétez les étapes 3 - 4 pour **WebSphere MQ** et **DataPower Appliance**. Ajoutez les autres instances IBM Integration Bus, IBM MQ et dispositif DataPower jusqu'à ce que la Pile d'intégration IBM soit terminée.



6. Cliquez sur **Fermer**, puis sur **Sauvegarder** pour revenir au Tableau de bord d'Application Performance.

Résultats

Conseil : Si le tableau de bord Agréger une topologie de transaction ne contient pas la topologie attendue, attendez que celui-ci s'actualise, puis vérifiez de nouveau quelques minutes plus tard. Si la topologie ne correspond toujours pas à vos attentes, votre application ne communique peut-être pas avec les composants attendus. Vérifiez votre environnement.

Affichage des résultats de la surveillance de la Pile d'intégration IBM

Vous pouvez afficher les résultats de la surveillance de la Pile d'intégration IBM dans les pages de topologies et de middleware. Vous pouvez également afficher les événements générés lorsqu'une transaction dépasse un seuil défini.

Pourquoi et quand exécuter cette tâche

Les topologies affichent les interactions entre les composants de middleware. Les noeuds middleware suivants s'affichent dans Agréger une topologie de transaction et Topologie des instances de transaction :

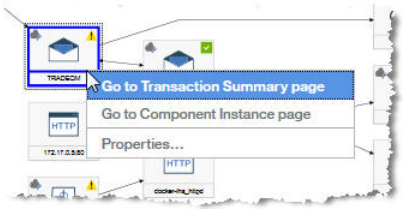
- IBM Integration Bus
- IBM MQ
- dispositif DataPower

Faites glisser le pointeur de la souris sur un noeud pour afficher une fenêtre de propriétés qui fournit des informations expliquant pourquoi un noeud a un statut particulier. Le statut est déterminé par des situations ; les situations dont le statut est incorrect sont affichées.

Procédure

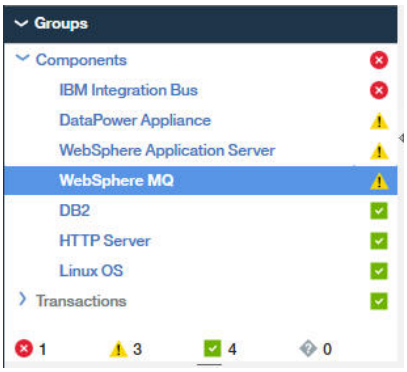
Vous pouvez créer un lien entre les noeuds de la topologie et les détails supplémentaires sur ce noeud :

1. Cliquez sur un noeud avec le bouton droit de la souris.



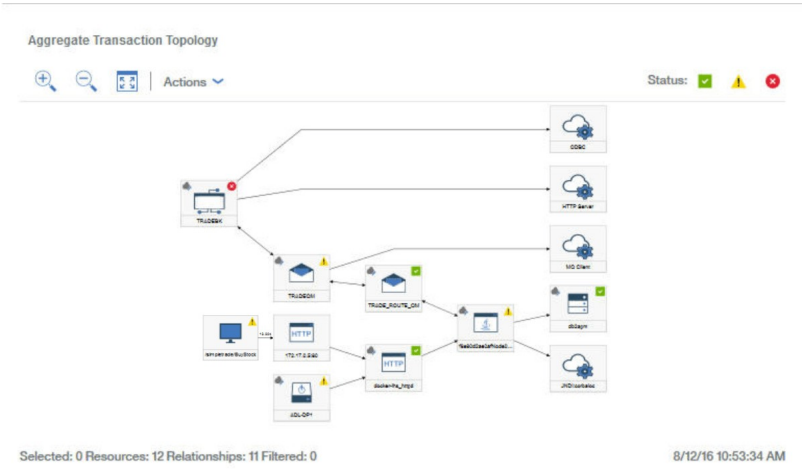
2. Facultatif : Sélectionnez **Accéder à la page Instance de composant** pour afficher des informations sur le composant.
3. Facultatif : Sélectionnez **Accéder à la page Récapitulatif des transactions** pour afficher des informations sur les transactions de middleware.

   Conseil : Sélectionnez **Groupes** > **Composants** > *composant middleware* dans le navigateur et sélectionnez une période de demande dans le widget de volume pour accéder au même tableau de bord.



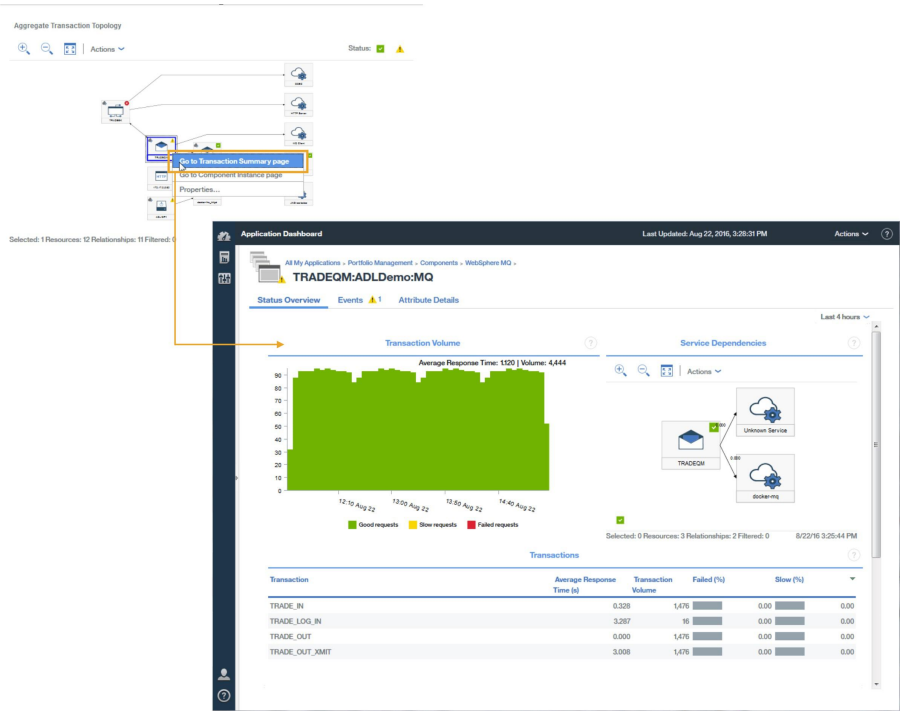
Agréger une topologie de transaction

Le widget Agréger une topologie de transaction est affiché dans le tableau de bord Récapitulatif de l'application.



Le widget Agréger une topologie de transaction peut afficher les noeuds IBM MQ, IBM Integration Bus et dispositif DataPower. Effectuez une exploration en aval à partir de ces noeuds pour obtenir plus d'informations sur la pile d'intégration du middleware.

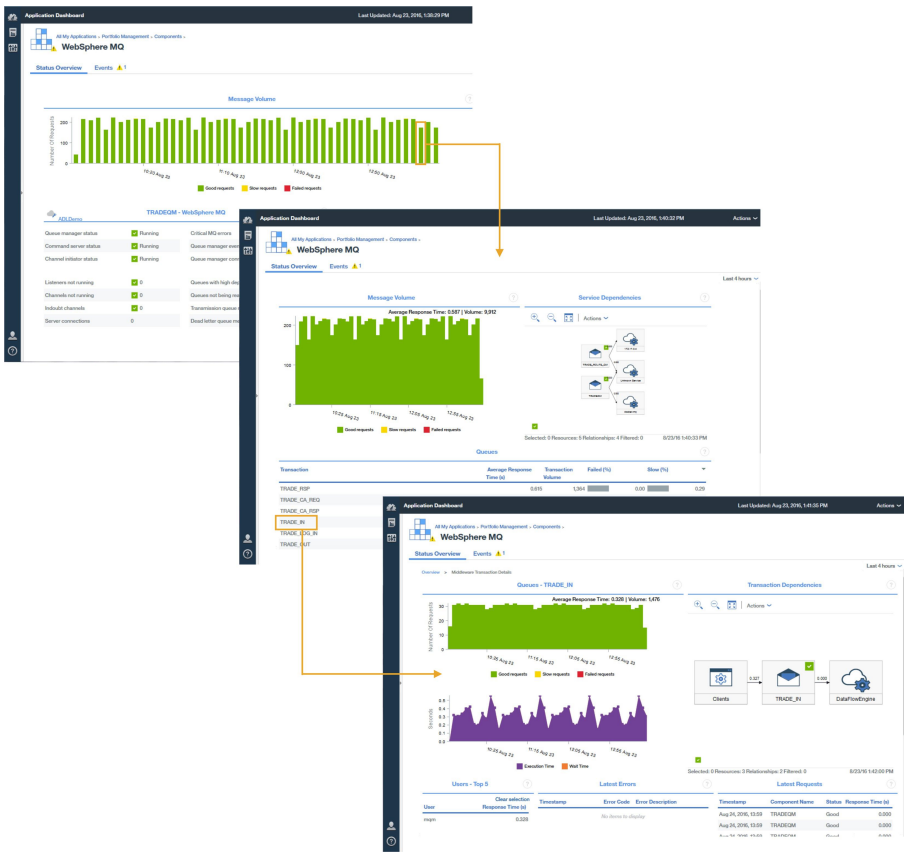
Pour explorer en aval, cliquer sur un noeud de middleware avec le bouton droit de la souris dans Agréger une topologie de transaction, puis sélectionnez **Accéder à la page Récapitulatif des transactions**. Vous pouvez également sélectionner **Groupes** > **Composants** > *composant de middleware* dans le navigateur et sélectionner une période de demande dans le widget de volume pour accéder aux mêmes informations.



Détails des transactions de middleware

A partir de la page Récapitulatif des transactions de middleware, vous pouvez explorer en aval jusqu'aux détails des transactions de middleware.

Pour explorer en aval les détails des transactions de middleware pour le composant, procédez comme suit :



1. Dans la page Récapitulatif des transactions de middleware pour le composant, sélectionnez un intervalle de surveillance dans le graphique Message ou volume.
2. Dans la page Récapitulatif des transactions de middleware, dans le widget **Files d'attente**, **Courtiers** ou **Dispositifs**, sélectionnez une file d'attente, un courtier ou un dispositif.

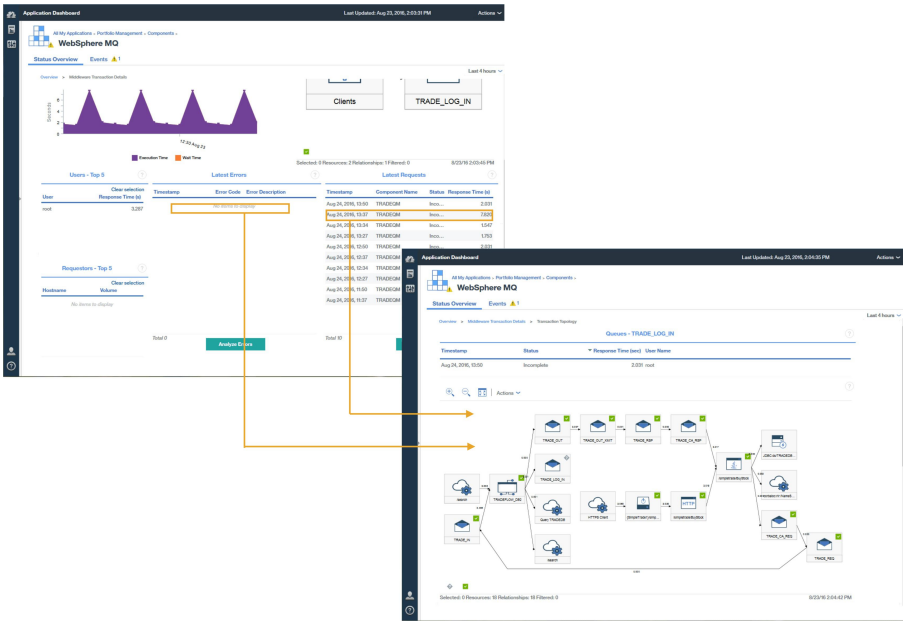
Analyse des erreurs et des instances

A partir de la page de détails des transactions du middleware, vous pouvez effectuer une exploration en aval jusqu'aux informations qui vous aident à analyser les erreurs et instances et accéder à la topologie des instances de transaction.

Pour explorer en aval jusqu'aux erreurs et instances des composants de middleware, puis accéder à la topologie des instances de transaction, dans la page Détails des transactions, effectuez l'une des étapes suivantes :

- Cliquez sur **Erreurs d'analyse** pour afficher la page Analyse des erreurs, puis sélectionnez une erreur.
- Cliquez sur **Demandes d'analyse** pour afficher la page Analyse d'instance, puis sélectionnez une instance.

Vous pouvez également, dans la page Détails des transactions, sélectionner une erreur ou une instance pour accéder directement à la topologie des instances de transaction.



Les topologies des instances de transaction affichent les noeuds middleware suivants :

- Gestionnaires de files d'attente de messages
- Courtiers IBM Integration Bus
- Dispositifs DataPower

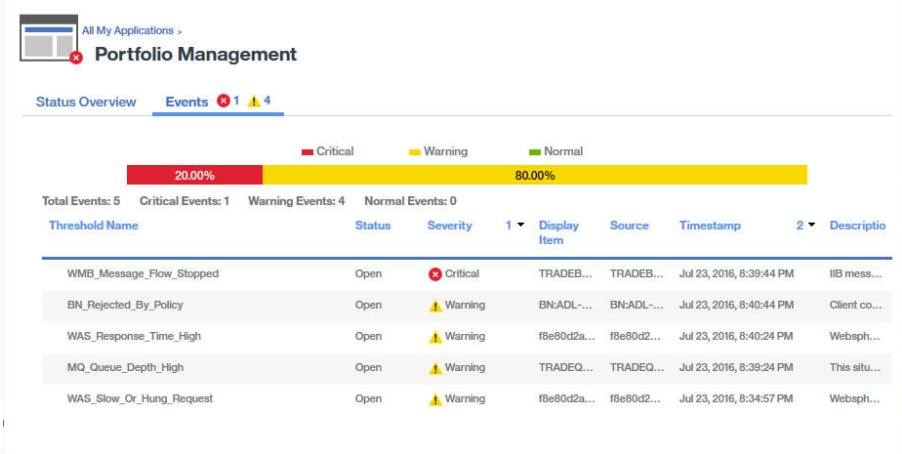
Sélectionnez un noeud pour afficher ses propriétés qui expliquent pourquoi un noeud a un statut particulier.

Un diagramme de Gantt des transactions s'affiche pour la file d'attente ou le courtier sélectionné. Le diagramme de Gantt vous aide à isoler les éléments les plus pertinents concernant le temps de réponse global de la transaction.



Evénements

Les seuils de suivi des transactions par défaut génèrent des événements pour la Pile d'intégration IBM, en plus des autres agents.



Pour plus d'informations sur les événements de suivi des transactions par défaut, voir «Seuils d'événement pour la surveillance des transactions», à la page 1045.

Vous pouvez ajouter des seuils pour créer plus d'événements, par exemple pour des débits de transaction qui sont lents ou qui passent au-dessous d'un certain seuil.

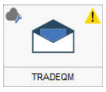
Pour plus d'informations sur l'ajout d'événements, voir «Création de seuils de génération d'événements pour la surveillance des transactions», à la page 1048.

Diagnostic des incidents de votre environnement

Si les instances de transaction de l'un des composants de votre environnement sont lentes ou en échec alors le statut approprié est affecté au composant impacté.

Un noeud peut avoir l'un des statuts suivants :

- 

Satisfaisant : le noeud est caractérisé par une coche entourée d'un carré vert qui s'affiche dans l'angle supérieur droit
- 

Avertissement : le noeud est caractérisé par un point d'exclamation entouré d'un triangle jaune qui s'affiche dans l'angle supérieur droit
- 

Critique : l'arrière-plan du noeud est rouge et une croix dans un cercle rouge s'affiche dans l'angle supérieur droit

Pour identifier la nature des problèmes liés aux composants dont le statut est avertissement ou critique, cliquez avec le bouton droit de la souris sur le noeud et examinez en détail les informations sur les causes probables des incidents.

Chapitre 6. Instructions de téléchargement

Téléchargez les images d'installation d'IBM Cloud Application Performance Management à partir du site Web d'IBM Passport Advantage.

Les images d'installation sont disponibles pour les composants Performance Management, les packs d'extension et les produits Tivoli Monitoring en offre groupée sous la forme d'un ensemble d'images pour chaque type d'offre.

Composants Cloud APM, Private

Examinez les descriptions des images IBM Cloud Application Performance Management, Private pour identifier les composants à télécharger.

Les offres Cloud APM, Private possèdent un ensemble d'images de composant téléchargeables. Téléchargez les images relatives à votre offre.

Important : Ne modifiez pas le nom du fichier image d'installation des agents ou de la Passerelle hybride pendant ou après le téléchargement à moins de vous conformer aux impératifs suivants : le nouveau nom n'excède pas 40 caractères et contient le mot «agents» ou «hybrid_gateway» du nom d'origine. Sinon les outils de configuration ne reconnaissent pas le fichier et la configuration échoue.

serveur Cloud APM

- Image 64 bits RHEL d'installation du serveur, qui inclut les composants serveur suivants :
  - Le serveur Cloud APM, y compris la base de données Db2, l'agent Summarization and Pruning, la base de données MongoDB et l'infrastructure d'offre d'agent.
    - La base de données Db2 stocke les informations sur les relations, les attributs et les ressources des agents dans SCR (Service Component Repository). La base de données de préextraction Db2 est un entrepôt de données pour les mesures des agents.
    - L'agent Summarization and Pruning est configuré et effectue les fonctions d'agrégation et d'élagage des données historiques dans la base de données Db2.
    - La base de données MongoDB stocke les données d'événement de seuil et de suivi des transactions.
    - L'infrastructure d'offre d'agent est installée dans le répertoire `AgentFrameworks` au cours de l'installation du serveur Cloud APM. L'infrastructure d'agent est injectée dans les images d'installation de l'agent pendant la configuration.
  - console Cloud APM, qui représente l'interface utilisateur des tableaux de bord.
  - Serveur d'aide KC-CI, qui prend en charge les systèmes d'aide des agents de surveillance et de la console Cloud APM.

Téléchargez et installez le serveur Cloud APM sur un système informatique ou une machine virtuelle où vous souhaitez que l'infrastructure de surveillance soit installée.

Pour des instructions sur l'installation du serveur Cloud APM et des composants de prise en charge, voir Chapitre 7, «Installation du serveur», à la page 125.

Agents Cloud APM

- Image d'installation des agents pour Linux 64 bits
- Image d'installation des agents pour AIX

Pour des instructions sur l'installation de ces agents, voir «Installation des agents sur les systèmes Linux», à la page 170 et «Installation des agents sur les systèmes AIX», à la page 165.

© Copyright IBM Corp. 2015, 2018

- Image d'installation des agents pour Windows 64 bits
- Image d'installation des agents pour Windows 32 bits

Pour des instructions sur l'installation de ces agents sur des systèmes Windows, voir «Installation des agents sur les systèmes Windows», à la page 177.

Pour télécharger les images d'agent, vous disposez de trois options :

- Téléchargez les images d'agent sur le système sur lequel vous avez téléchargé l'image d'installation du serveur Cloud APM. Les images d'agent peuvent être montées sur une partition NFS, mais elles doivent être accessibles à l'aide du système de fichiers. Vous pouvez configurer les images d'agent lorsque vous y êtes invité lors de l'installation du serveur et copiez les images configurées sur le système sur lequel les applications à surveiller sont installées.
- Téléchargez les images d'agent sur le système où les applications que vous souhaitez surveiller sont installées. Une fois que vous avez installé le serveur, créez des modules de configuration pour connecter les agents au serveur. Copiez les modules de configuration sur le système sur lequel vous avez téléchargé les images d'agent et configurez les images d'agent.
- Téléchargez les images d'agent sur n'importe quel système de votre environnement. Sur le système sur lequel vous avez installé le serveur, créez des modules de configuration pour connecter les agents au serveur. Copiez les modules de configuration sur le système sur lequel les images d'agent sont téléchargées, configurez les images d'agent et téléchargez-les sur le système sur lequel les applications à surveiller sont installées.

Les agents de surveillance sont autonomes et ne possèdent pas d'infrastructure autre que celle qui est fournie par le serveur Cloud APM pour le partage des données. L'impact sur les performances et sur la taille des noeuds individuels est faible. La conservation des données est locale et temporaire.

Collecteurs de données Cloud APM (disponibles uniquement dans Cloud APM, Advanced Private)

- Image de collecteurs de données pour AIX
- Image de collecteurs de données pour Linux
- Image de collecteurs de données pour Windows

Téléchargez les images de collecteur de données, configurez les images téléchargées pour la communication serveur, puis configurez le collecteur de données pour surveiller vos applications. Pour obtenir des instructions sur la configuration de l'image pour la communication serveur, voir «Configuration des images téléchargées», à la page 162. Pour des instructions sur la configuration du collecteur de données pour la surveillance, voir les sous-sections relatives aux applications concernées dans Chapitre 10, «Configuration de votre environnement», à la page 201.

Rapports Cloud APM

- Image des rapports Cloud APM, qui contient des rapports basés sur Cognos pour l'examen en détail des statistiques d'unité et des performances d'application.

Vous devez installer Tivoli Common Reporting avant d'installer l'image des rapports. Pour plus d'informations sur la version de Tivoli Common Reporting à installer et sur la configuration et l'installation des rapports Cloud APM, voir «Intégration à Tivoli Common Reporting», à la page 917.

Agent Builder

- Image d'Agent Builder, qui contient le kit d'outils d'Agent Builder pour la création d'agents personnalisés afin d'étendre les ressources que vous pouvez surveiller.
- Module linguistique d'Agent Builder.

Pour obtenir des instructions d'installation du kit d'outils autonome Agent Builder sur plusieurs plateformes, voir le document IBM Agent Builder - Guide d'utilisation.

Passerelle hybride

- Image de la Passerelle hybride, qui contient un composant pour les environnements comportant des agents IBM Tivoli Monitoring.

Si votre environnement inclut des produits IBM Tivoli Monitoring que vous souhaitez afficher dans console Cloud APM, vous pouvez télécharger et installer l'image de la Passerelle hybride d'IBM Cloud Application Performance Management. Vous disposez des mêmes options que pour les images d'agent pour télécharger et configurer l'image de la Passerelle hybride et vous pouvez télécharger la Passerelle hybride en même temps que les images d'agent et sur le même système. La seule différence tient au fait que la Passerelle hybride est installée dans votre environnement Tivoli Monitoring sur un seul système Red Hat Enterprise Linux (RHEL).
Pour obtenir des instructions sur l'installation de la Passerelle hybride, voir «Intégration à IBM Tivoli Monitoring V6.3», à la page 871.

Packs d'extension

Examinez les descriptions des images des packs d'extension afin d'identifier celles à télécharger pour votre offre.

Pour une liste des agents inclus dans chaque module d'extension, voir «Offres et modules complémentaires», à la page 35.

Advanced Extension Pack

(Non disponible pour Cloud APM, Base Private)

- Advanced Extension Pack pour Linux 64 bits
- Advanced Extension Pack pour Windows 64 bits
- Advanced Extension Pack pour AIX
- Monitoring Agent for SAP HANA Database version 7.1

Base Extension Pack

- Base Extension Pack pour Linux 64 bits
- Base Extension Pack pour Windows 64 bits
- Base Extension Pack pour AIX

Infrastructure Extension Pack

- Infrastructure Extension Pack pour Linux 64 bits
- Infrastructure Extension Pack pour Windows 64 bits

Pour des instructions sur le téléchargement des images, voir «Téléchargement depuis Passport Advantage», à la page 118. Pour obtenir des instructions sur l'installation des packs d'extension, voir Chapitre 9, «Installation des agents», à la page 161.

Produits regroupés avec Tivoli Monitoring

Les produits regroupés basés sur l'infrastructure IBM Tivoli Monitoring sont disponibles avec les offres IBM Cloud Application Performance Management.

Examinez les instructions pour déterminer le produit regroupé avec Tivoli Monitoring à installer avec votre offre.

Si aucun des produits regroupés avec Tivoli Monitoring n'est installé, installez les composants Cloud APM.

Si vous utilisez actuellement l'un des produits Tivoli Monitoring inclus, suivez ces instructions :

- Si des agents basés sur Tivoli Monitoring sont déjà installés sur un système (virtuel ou physique) et que vous souhaitez installer d'autres agents, vous pouvez utiliser les agents basés sur Tivoli Monitoring

ou les agents Cloud APM. Grâce à la fonction de coexistence des agents, vous pouvez installer les agents Cloud APM sur le même système que les agents Tivoli Monitoring, mais pas dans le même répertoire.

- Si vous souhaitez surveiller des systèmes sur lesquels aucun des agents basés sur Tivoli Monitoring n'est actuellement installé, vous pouvez utiliser les agents IBM Tivoli Monitoring ou les agents Cloud APM.

S'il n'existe pas d'agent Cloud APM pour le système d'exploitation ou le middleware que vous souhaitez surveiller, installez l'agent Tivoli Monitoring et l'infrastructure Tivoli Monitoring.

Connectez les agents Tivoli Monitoring à l'infrastructure Tivoli Monitoring et les agents Cloud APM à l'infrastructure Cloud APM. Si les composants du serveur Cloud APM et de la Passerelle hybride sont installés, vous pouvez afficher les ressources surveillées de vos domaines Tivoli Monitoring et Cloud APM dans les mêmes tableaux de bord sur la console Cloud APM. Pour connaître la liste des agents Tivoli Monitoring disponibles par le biais de la Passerelle hybride, voir le Hybrid Gateway supported agents (APM Developer Center).

La liste des produits en offre groupée Tivoli Monitoring disponibles avec chaque offre est indiquée dans tableau 21, à la page 122 à la rubrique *Numéros de référence*. Pour des instructions sur le téléchargement des images, voir «Téléchargement depuis Passport Advantage».

Téléchargement depuis Passport Advantage

Vous pouvez acheter et télécharger le logiciel et la licence de production depuis IBM Passport Advantage.

Pourquoi et quand exécuter cette tâche

Reportez-vous à la lettre d'annonce IBM Cloud Application Performance Management, Private pour connaître les informations sur la licence (voir IBM Offering Information).

Pour obtenir de l'aide pour IBM Passport Advantage, recherchez «support passport advantage» dans votre navigateur et sélectionnez le lien «Contact us» ou rendez-vous sur IBM Passport Advantage - Contact us.

Procédure

1. Identifiez les composants Cloud APM que vous voulez télécharger. Pour une description des images du composant, voir «Composants Cloud APM, Private», à la page 115.
2. Identifiez les modules d'extension Cloud APM que vous voulez télécharger. Pour une description des images des packs d'extension, voir «Packs d'extension», à la page 117.
3. Identifiez les produits Tivoli en offre groupée que vous voulez télécharger. Pour une description des images du produit Tivoli, voir «Produits regroupés avec Tivoli Monitoring», à la page 117.
4. Localisez les numéros de référence eAssembly et eImage associés dans la rubrique «Numéros de référence».
5. Accédez au site Web d'IBM Passport Advantage, connectez-vous, puis recherchez les numéros de référence.
6. Téléchargez les images.

Numéros de référence

Examinez les numéros de référence afin d'identifier les composants à télécharger pour votre installation de IBM Cloud Application Performance Management, Private V8.1.4.

IBM Cloud Application Performance Management, Private, composants

Les numéros de référence et les noms de fichier des composants Cloud APM, Private sont indiqués dans le tableau 15.

Tableau 15. Noms de fichier des composants d'Cloud APM, Private, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage

Descriptions des composants eImage	Cloud APM, Advanced Private (CJ25SML)	Cloud APM, Base Private (CJ25GML)
Fichier tar d'installation du serveur	CNM44ML advanced_8.1.4.0.tar	CNM43ML base_8.1.4.0.tar
Fichiers tar d'installation d'agent pour Linux for System x	CNUL2ML advanced_agents_xlinux_8.1.4.0.5.tar	CNUM8ML base_agents_xlinux_8.1.4.0.5.tar
Fichiers tar d'installation d'agent pour Linux on System z	CNUL6ML advanced_agents_zlinux_8.1.4.0.5.tar	CNUN0ML base_agents_zlinux_8.1.4.0.5.tar
Fichiers tar d'installation d'agent pour pLinux LE	CNUL7ML advanced_agents_plinuxle_8.1.4.0.5.tar	CNUN1ML base_agents_plinuxle_8.1.4.0.5.tar
Fichier tar d'installation des agents pour les systèmes AIX	CNUL4ML advanced_agents_aix_8.1.4.0.5.tar	CNUM9ML base_agents_aix_8.1.4.0.5.tar
Fichier zip d'installation des agents pour les systèmes Windows 64 bits	CNUL3ML advanced_agents_win_8.1.4.0.5.zip	CNUM6ML base_agents_win_8.1.4.0.5.zip
Fichier zip d'installation des agents pour les systèmes Windows 32 bits	CNUL5ML advanced_agents_win32_8.1.4.0.5.zip	CNUM7ML base_agents_win32_8.1.4.0.5.zip
Fichier tar d'installation du kit d'outils Agent Builder pour plusieurs plateformes	CNL8RML ibm_agent_builder_6.3.5.tar	CNL8RML ibm_agent_builder_6.3.5.tar
Module de langues Agent Builder	CNL8QML ibm_agent_builder_langpack_6.3.5.tar	CNL8QML ibm_agent_builder_langpack_6.3.5.tar
Fichier tar d'installation de la passerelle hybride	CNL8SML apm_hybrid_gateway_8.1.4.0.tar	CNL8SML apm_hybrid_gateway_8.1.4.0.tar

Tableau 15. Noms de fichier des composants d'Cloud APM, Private, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage (suite)

Descriptions des composants eImage	Cloud APM, Advanced Private (CJ25SML)	Cloud APM, Base Private (CJ25GML)
Rapports Cloud APM(Le programme d'installation de rapports Cloud APM nécessite Java 8 pour installer les rapports.)	CNM45ML apm_advanced_reports_8.1.4.0.zip	CNM42ML apm_base_reports_8.1.4.0.zip
Collecteurs de données pour Windows	CNUL8ML _datacollectors_win_8.1.4.0.5.zip	N/A
Collecteurs de données pour Linux	CNUL9ML _datacollectors_linux_8.1.4.0.5.tgz	N/A
Collecteurs de données pour AIX	CNUM0ML _datacollectors_aix_8.1.4.0.5.tgz	N/A

Packs d'extension disponibles avec IBM Cloud Application Performance Management, Advanced Private

Les numéros de référence et les noms de fichier de l'offre Cloud APM, Advanced Private Advanced Extension Pack sont indiqués dans le tableau 16.

Tableau 16. Noms de fichier Advanced Extension Pack, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage

Descriptions des composants eImage	Cloud APM, Advanced Private Advanced Extension Pack (CJ25TML)
Fichier tar de l'offre Advanced Extension Pack pour les systèmes Linux 64 bits	CNUM1ML advanced_extension_xlinux_8.1.4.0.5.tar
Fichier tar de l'offre Advanced Extension Pack pour les systèmes AIX	CNUM3ML advanced_extension_aix_8.1.4.0.5.tar
Fichier zip de l'offre Advanced Extension Pack pour les systèmes Windows 64 bits	CNUM2ML advanced_extension_win_8.1.4.0.5.zip
Fichier tar de l'agent de surveillance IBM pour SAP HANA Database v7.1 pour les plateformes Linux 64 bits, Windows 64 bits et AIX	CNAM8ML ipm_sap_ext_agents_V71.tar
IBM Monitoring Agent for SAP HANA Database V7.1.1 Multilingual pour les plateformes Linux 64 bits, Windows 64 bits et AIX	CNUM4ML CNUM4ML.tar.gz
IBM Monitoring Agent for SAP HANA Database V7.1.1 Language Pack pour les plateformes Linux 64 bits, Windows 64 bits et AIX	CNUM5ML CNUM5ML.tar

Les numéros de référence et les noms de fichier de l'offre Cloud APM, Advanced Private Base Extension Pack sont indiqués dans le tableau 17.

Tableau 17. Noms de fichier Base Extension Pack, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage

Descriptions des composants eImage	Cloud APM, Advanced Private Base Extension Pack (CJ25HML)
Fichier tar de l'offre Base Extension Pack pour les systèmes Linux 64 bits	CNUN2ML base_extension_xlinux_8.1.4.0.5.tar
Fichier tar de l'offre Base Extension Pack pour les systèmes AIX	CNUN4ML base_extension_aix_8.1.4.0.5.tar
Fichier zip de l'offre Base Extension Pack pour les systèmes Windows 64 bits	CNUN3ML base_extension_win_8.1.4.0.5.zip
IBM Monitoring Agent for Hadoop V7.10.0.0 pour les plateformes Linux 64 bits, Windows 64 bits et AIX	CNUN5ML CNUN5ML.tar
IBM Monitoring Agent for Hadoop V7.10.0.0 Language Pack pour les plateformes Linux 64 bits, Windows 64 bits et AIX	CNUN6ML CNUN6ML.tar

Les numéros de référence et les noms de fichier de l'offre Cloud APM, Advanced Private Infrastructure Extension Pack sont indiqués dans le tableau 18.

Tableau 18. Noms de fichier Infrastructure Extension Pack, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage

Descriptions des composants eImage	Cloud APM, Advanced Private Infrastructure Extension Pack (CJ25IML)
Fichier tar de l'offre Infrastructure Extension Pack pour les systèmes Linux 64 bits	CNUN7ML apm_infra_agents_xlinux_8.1.4.0.5.tar
Fichier zip de l'offre Infrastructure Extension Pack pour les systèmes Windows 64 bits	CNUN8ML apm_infra_agents_win_8.1.4.0.5.zip

Packs d'extension disponibles avec IBM Cloud Application Performance Management, Base Private

Les numéros de référence et les noms de fichier de l'offre Cloud APM, Base Private Base Extension Pack sont indiqués dans le tableau 19.

Tableau 19. Noms de fichier Base Extension Pack, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage

Descriptions des composants eImage	Cloud APM, Base Private Base Extension Pack (CJ25HML)
Fichier tar de l'offre Base Extension Pack pour les systèmes Linux 64 bits	CNUN2ML base_extension_xlinux_8.1.4.0.5.tar
Fichier tar de l'offre Base Extension Pack pour les systèmes AIX	CNUN4ML base_extension_aix_8.1.4.0.5.tar
Fichier zip de l'offre Base Extension Pack pour les systèmes Windows 64 bits	CNUN3ML base_extension_win_8.1.4.0.5.zip

Les numéros de référence et les noms de fichier de l'offre Cloud APM, Base Private Infrastructure Extension Pack sont indiqués dans le tableau 20.

Tableau 20. Noms de fichier Infrastructure Extension Pack, numéros de référence des composants eAssembly (entre parenthèses) et numéros de référence des composants eImage

Descriptions des composants eImage	Cloud APM, Base Private Infrastructure Extension Pack (CJ25IML)
Fichier tar de l'offre Infrastructure Extension Pack pour les systèmes Linux 64 bits	CNUN7ML `apm_infra_agents_xlinux_8.1.4.0.5.tar`
Fichier zip de l'offre Infrastructure Extension Pack pour les systèmes Windows 64 bits	CNUN8ML `apm_infra_agents_win_8.1.4.0.5.zip`

Produits en offre groupée avec IBM Tivoli Monitoring

Une fois que vous avez acheté votre licence Cloud APM, Private, vous pouvez télécharger l'ensemble ou une partie des logiciels regroupés avec Tivoli Monitoring. Les numéros de référence des composants eAssembly pour les produits regroupés avec Tivoli Monitoring qui sont disponibles avec votre offre sont répertoriés dans le tableau 21.

Vous devez connecter les agents Tivoli Monitoring à l'infrastructure Tivoli Monitoring. Les données de ces agents sont visualisables dans la console Cloud APM uniquement si vous installez le serveur Cloud APM et les composants de la Passerelle hybride et si les agents sont disponibles par le biais de la Passerelle hybride. Pour obtenir la liste des agents pris en charge par la passerelle hybride, voir Hybrid Gateway supported agents (APM Developer Center).

Tableau 21. Numéros de référence des composants eAssembly pour les produits regroupés avec IBM Tivoli Monitoring téléchargeables à partir du site Passport Advantage à utiliser avec l'offre IBM Cloud Application Performance Management

Titre dans Passport Advantage	Cloud APM, Advanced Private	Cloud APM, Base Private	Documentation du produit
IBM Operations Analytics Log Analysis for *nom_offre*	CJ25WML	CJ25JML	Cliquez ici
IBM SmartCloud Application Performance Management Standard & Non-Prod version 7.7 for *nom_offre*	CJ25XML	N/A	Cliquez ici
IBM SmartCloud Application Performance Management Entry Edition for IBM Monitoring	N/A	CJ25KML	Cliquez ici
IBM Rational 8.6 for IBM Tivoli Composite Application Manager Transactions version 7.4 for *nom_offre*	CJ260ML	N/A	Cliquez ici
IBM Tivoli Composite Application Manager for Applications for *nom_offre*	CJ261ML	CJ25QML	Cliquez ici
IBM Tivoli Composite Application Manager for Application Diagnostics 7.1.0.4 for *nom_offre*	CRW72ML	N/A	Cliquez ici
IBM Tivoli Composite Application Manager for Microsoft Applications for *nom_offre*	CJ262ML	CJ25MML	Cliquez ici
IBM Tivoli Composite Application Manager for Transactions for *nom_offre*	N/A	CJ25LML	Cliquez ici

Tableau 21. Numéros de référence des composants eAssembly pour les produits regroupés avec IBM Tivoli Monitoring téléchargeables à partir du site Passport Advantage à utiliser avec l'offre IBM Cloud Application Performance Management (suite)

Titre dans Passport Advantage	Cloud APM, Advanced Private	Cloud APM, Base Private	Documentation du produit
IBM Tivoli Composite Application Manager Transactions V7.4 Response Time and Internet Service Monitoring for *nom_offre*	CJ25YML	N/A	Cliquez ici
IBM Tivoli Monitoring for *nom_offre*	CJ263ML	CJ25NML	Cliquez ici
IBM Tivoli Composite Application Manager Transactions version 7.4 Transaction Tracking for *nom_offre*	CJ25ZML	N/A	Cliquez ici
IBM Tivoli Monitoring for Virtual Environments for *nom_offre*	CJ264ML	CJ25PML	Cliquez ici
IBM Db2 Enterprise Server Edition 10.1 for IBM Tivoli Composite Application Manager for Application Diagnostics V7.1.0.4	CRW7SML	N/A	Cliquez ici
IBM WebSphere Application Server 8.5.5 for IBM Tivoli Composite Application Manager for Application Diagnostics version 7.1.0.4 for Multiplatform Multilingual	CJ265ML	N/A	Cliquez ici

Si vous prévoyez d'intégrer Tivoli Common Reporting à Cloud APM, vous pouvez accéder à Tivoli Common Reporting v3.1.2.1 en installant Jazz for Service Management v1.1.2.0 et en effectuant une mise à niveau vers le groupe de correctifs 1. Jazz for Service Management est disponible avec Tivoli Monitoring. Le tableau 22 répertorie les numéros de référence eImage de Jazz for Service Management.

Tableau 22. Numéros de référence eImage pour Jazz for Service Management v1.1.2.0

Titre dans Passport Advantage	Numéro de référence eImage
Jazz for Service Management V1.1.2.0 Quick Start Guide Multilingual	CN54TML
Jazz for Service Management V1.1.2.0 for AIX Multilingual	CN54UML
Jazz for Service Management V1.1.2.0 for Linux Multilingual	CN54VML
Jazz for Service Management V1.1.2.0 for Linux on System z Multilingual	CN54WML

Chapitre 7. Installation du serveur

Le serveur Cloud APM et les composants de prise en charge fournissent l'infrastructure de surveillance avec console Cloud APM.

Installez le serveur Cloud APM comme première étape de configuration de votre environnement IBM Cloud Application Performance Management.

Le serveur Cloud APM doit être installé par un superutilisateur sur une version prise en charge de Red Hat Enterprise Linux.

Une fois le serveur Cloud APM installé, vous ne pouvez pas modifier les droits d'accès des fichiers et des répertoires de Cloud APM, ni modifier les propriétaires de groupe ou d'utilisateur de ces fichiers et répertoires.

Pour obtenir une liste des systèmes d'exploitation pris en charge, voir le rapport de compatibilité du produit logiciel relatif à votre offre. Les liens vers ces rapports se trouvent dans le document System requirements (APM Developer Center).

Si vous avez téléchargé les images des agents de surveillance, vous pouvez les configurer dans le cadre de la procédure d'installation de l'infrastructure de surveillance. Si vous avez l'intention d'effectuer la surveillance avec les agents de votre environnement IBM Tivoli Monitoring, vous pouvez également télécharger l'image de la Passerelle hybride d'IBM Cloud Application Performance Management et configurer cette image dans le cadre de la procédure d'installation.

Préparation de l'installation du serveur

Pour surveiller votre environnement, vous devez commencer par installer le serveur Cloud APM et les composants de prise en charge.

Passez en revue les options et les exigences afin de vous aider à planifier votre installation du serveur Cloud APM.

Composants installés avec le serveur Cloud APM

Le processus d'installation installe également un serveur Db2, un Agent Summarization and Pruning et une base de données MongoDB sur le même système que le serveur Cloud APM. La base de données Db2 stocke les définitions d'application et les données de relation et de mesure. La base de données MongoDB stocke les données d'événement de seuil et de suivi des transactions.

Exigences et systèmes d'exploitation pris en charge

Vous devez disposez des droits de superutilisateur pour installer et exécuter le serveur Cloud APM. L'exécution du serveur Cloud APM en tant qu'utilisateur non superutilisateur n'est pas prise en charge.

Consultez les rubriques Chapitre 4, «Configuration requise», à la page 71 et Dépendances pour connaître les systèmes d'exploitation pris en charge et les exigences relatives au serveur Cloud APM.

Configuration des images téléchargées lors de l'installation du serveur

Avant d'installer les agents et la Passerelle hybride d'IBM Cloud Application Performance Management, ou de configurer le collecteur de données, vous devez configurer les images téléchargées pour initier la communication avec le serveur Cloud APM. Les images téléchargées

© Copyright IBM Corp. 2015, 2018

peuvent être configurées automatiquement lors de l'installation du serveur si vous téléchargez les images sur le système sur lequel le serveur va être installé.

Les images téléchargées peuvent être montées sur une partition NFS, mais elles doivent être accessibles à l'aide du système de fichiers. Ne modifiez pas le nom des fichiers image d'installation au cours ou après le téléchargement. Si le nom d'un fichier image d'installation est modifié, il n'est pas reconnu par les outils de configuration d'image et la configuration échoue. Pour plus d'informations, voir Chapitre 6, «Instructions de téléchargement», à la page 115.

Configuration de votre programme d'analyse antivirus afin d'exclure les fichiers de base de données Db2
Si vous utilisez un programme d'analyse antivirus, comme McAfee Virus Scan for Linux ou Sophos, vous devez le configurer pour exclure tous les fichiers de base de données Db2, y compris les groupes de stockage, les espaces de table et les pools de mémoire tampon. Configurez le programme d'analyse antivirus avant d'installer le serveur Cloud APM. Les fichiers de base de données Db2 sont installés dans le répertoire *rép_install*/db2 par défaut, par exemple /opt/ibm/db2.

Création d'utilisateurs Db2 avant l'installation du serveur Cloud APM
L'installation du serveur Cloud APM crée un serveur Db2 sur votre système local. Plusieurs utilisateurs d'instance et groupes Db2 sont créés lors de l'installation et chaque utilisateur est affecté à son groupe respectif. Pour respecter les règles d'administration de serveur de base de données de votre organisation, vous pouvez créer les utilisateurs d'instance Db2 avant que le serveur Db2 ne soit installé. Pour plus d'informations, voir «Création d'utilisateurs Db2 avant la connexion à un serveur Db2 local», à la page 140.

Connexion à un serveur Db2 distant
Si vous disposez d'un serveur Db2 distant, vous pouvez l'utiliser pour les bases de données du serveur Cloud APM au lieu d'installer le serveur Db2 local par défaut avec le serveur Cloud APM.

Vous pouvez souhaiter vous connecter à un serveur Db2 distant sur un système externe pour vous conformer aux règles d'administration de serveur de base de données de votre organisation. La connexion à un serveur Db2 distant permet également de réduire la charge sur le serveur Cloud APM, ce qui améliore les performances. Prévoyez d'utiliser une configuration Db2 distante lorsque les performances d'entrée-sortie de disque requises ne peuvent pas être obtenues sur le matériel attribué à votre serveur Cloud APM.

Le programme d'installation de Db2 crée l'utilisateur dasuser1 et le groupe dasadm1, puis affecte l'utilisateur dasuser1 au groupe dasadm1. Vous devez créer manuellement tous les autres utilisateurs et groupes et affecter les utilisateurs aux groupes appropriés.

Pour plus d'informations, voir «Connexion à un serveur Db2 distant», à la page 129.

Installation de MongoDB sur un système distant

A des fins d'évolutivité, vous pouvez installer MongoDB sur un autre système. Pour plus d'informations, voir «Installation d'une base de données MongoDB distante», à la page 152.

Installation du serveur Cloud APM sur un système informatique où l'authentification LDAP est utilisée

Si le système sur lequel vous prévoyez d'installer le serveur Cloud APM avec un serveur Db2 local utilise un service d'annuaire externe avec LDAP pour l'authentification d'utilisateur, vous devez mettre à jour les mots de passe de l'utilisateur itmuser et de l'utilisateur de l'instance Db2, si ceux-ci sont configurés dans votre service d'annuaire. Vous devez mettre à jour ces mots de passe avant d'installer le serveur Cloud APM. Après avoir installé le serveur Cloud APM, vous devez configurer le plug-in de sécurité LDAP sur le serveur Db2 local. Pour plus d'informations, voir «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.

Si vous prévoyez d'utiliser l'authentification LDAP transparente sur le système sur lequel vous installez le serveur Cloud APM, vous devez utiliser un serveur Db2 distant au lieu d'installer le

serveur Db2 en local avec leserveur Cloud APM. Pour plus d'informations, voir «Connexion à un serveur Db2 distant», à la page 129 et Prise en charge de la recherche de groupes et de l'authentification LDAP.

OIDC OpenID Connect (OIDC) est un protocole d'identité simple sur OAuth 2.0. OIDC est activé dans la console Cloud APM. OIDC permet à une application client de demander l'identité de l'utilisateur en tant que jeton d'ID d'une manière normalisée, similaire à REST. En outre, l'application client peut utiliser des jetons d'accès pour accéder à des services similaires à REST.

Un certificat autosigné est créé pour OIDC pendant l'installation. Vous pouvez configurer un certificat autosigné ou un certificat signé par une autorité de certification pour OIDC. Pour plus d'informations, voir «Configuration des certificats à l'aide d'une autorité de certification racine tierce», à la page 1033et«Configuration des certificats à l'aide d'une autorité de certification racine privée», à la page 1031.

Remplacement de Cloud APM, Base par l'offre Cloud APM, Advanced

Vous pouvez remplacer Cloud APM, Base par l'offre Cloud APM, Advanced à tout moment après avoir installé l'offre Cloud APM, Base ou effectué une mise à niveau vers l'offre Cloud APM, Base. Le remplacement de Cloud APM, Base par Cloud APM, Advanced peut prendre plus de temps que la simple installation de Cloud APM, Advanced. Pour plus d'informations, voir «Passage d'une offre à une autre», à la page 138.

APMUI

APMUI est le composant de console Cloud APM qui gère les demandes entrantes de l'interface utilisateur. Elle est basée sur WebSphere Liberty. Le fichier `server.xml` contient une instruction include pour `user-exit.xml`. Toutes les personnalisations doivent être effectuées dans `user-exit.xml` de sorte qu'elles ne se perdent pas lors d'une mise à niveau.

Configuration du pare-feu pour les demandes entrantes sur le serveur

Avant d'installer le serveur Cloud APM, vous pouvez vouloir désactiver temporairement votre pare-feu ou configurer les ports pour les demandes entrantes et sortantes.

Avant de commencer

Les connexions TCP sont lancées à partir des agents de surveillance, utilisateurs d'API et utilisateurs de la console Cloud APM vers le serveur Cloud APM. Le serveur Cloud APM peut également lancer des connexions TCP vers d'autres serveurs, par exemple des serveurs de base de données. Par conséquent, un pare-feu doit autoriser le lancement de la connexion TCP et la fourniture d'une réponse.

Procédure

Effectuez l'une des opérations suivantes pour ouvrir des ports ou désactiver le pare-feu :

- Configurez votre pare-feu pour les demandes entrantes sur les ports utilisés par le serveur Cloud APM et pour les demandes sortantes lancées par le serveur Cloud APM. Vérifiez que les ports indiqués dans le tableau 8, à la page 86 sous «Ports serveur Cloud APM», à la page 86 sont libres (c'est-à-dire qu'aucune application ne les écoute).
- Désactivez votre pare-feu en exécutant les commandes Red Hat Linux suivantes :

```
service iptables stop
chkconfig iptables off
```

Pour Red Hat Linux version 7.4, désactivez votre par-feu en exécutant les commandes suivantes :

```
service firewalld stop
systemctl disable firewalld
```

Que faire ensuite

Installez le serveur Cloud APM et les agents de surveillance.

Définition des communications HTTP ou HTTPS

Le protocole de communication par défaut entre le serveur Cloud APM et les agents est HTTP. Avant d'installer le serveur, vous pouvez utiliser une variable d'environnement pour définir le protocole HTTPS afin d'établir des communications sécurisées entre le serveur et les agents de surveillance.

Avant de commencer

- Les communications entre le serveur et les agents doivent utiliser le protocole HTTP ou HTTPS de manière cohérente.
- Si vous configurez les images d'agent lors de l'installation du serveur, le protocole de communication des agents est défini afin de correspondre à celui du serveur. Toutefois, si vous choisissez de configurer les images d'agent ultérieurement, veillez à définir le protocole de communication avec le paramètre utilisé par le serveur.
- Si vous modifiez le protocole utilisé par le serveur pour communiquer avec les agents de surveillance, vous devez également modifier le protocole utilisé par le serveur pour communiquer avec les agents de serveur. Pour plus d'informations, voir «Configuration du protocole de communications pour les agents de serveur», à la page 1097.
- Le magasin de clés serveur Cloud APM utilisé pour la communication HTTPS avec les agents est le même que celui utilisé par le réexpéditeur SMTP pour la communication SSL avec le serveur SMTP. Si un magasin de clés est créé et qu'un certificat de l'autorité de certification a été ajouté pour le réexpéditeur SMTP, vous devez rajouter le certificat de l'autorité de certification SMTP au nouveau magasin de clés. Pour des instructions, voir Gestionnaire d'événements dans «Configuration avancée», à la page 1117.
- Vous risquez de constater une baisse de performances si le protocole HTTPS est utilisé, en fonction du nombre d'agents de surveillance que vous exécutez.

Procédure

Avant d'installer le serveur Cloud APM, effectuez l'étape suivante pour modifier le protocole de communication :

Sur le système sur lequel vous prévoyez d'installer le serveur, entrez l'une des commandes suivantes :

- Pour définir le protocole de communication HTTPS (sécurisé) : `export APM_SECURE_COMMUNICATION=y`
- Pour définir le protocole de communication HTTP (non sécurisé) : `export APM_SECURE_COMMUNICATION=n` (A moins que la variable d'environnement APM_SECURE_COMMUNICATION n'ait été utilisée pour définir HTTPS, cette étape n'est pas nécessaire car le protocole par défaut est HTTP. Ainsi, lorsque vous utilisez une session shell vierge, par exemple, juste après vous être connecté, vous pouvez lancer l'installation du serveur pour établir les communications HTTP.)

Que faire ensuite

- Exécutez le script d'installation pour commencer à installer le serveur.

Tâches associées:

«Téléchargement et installation du serveur», à la page 141
Avant d'installer les agents de surveillance ou la Passerelle hybride ou de configurer les collecteurs de données, installez le serveur Cloud APM sur une machine virtuelle ou un ordinateur de votre réseau exécutant Red Hat Enterprise Linux.

«Configuration des certificats entre le serveur et les agents», à la page 222
Pour permettre les communications entre le serveur Cloud APM et les agents, vous pouvez configurer des certificats par défaut, personnalisés ou autosignés.

«Configuration du protocole de communications pour les agents de serveur», à la page 1097
Le protocole HTTP ou HTTPS est utilisé pour communiquer entre le serveur Cloud APM et les agents de serveur. Le serveur Cloud APM autorise les connexions à partir des agents de serveur qui s'authentifient à l'aide d'un certificat valide. Si vous modifiez le protocole de communication utilisé par le serveur pour communiquer avec les agents de surveillance, vous devez modifier le protocole utilisé par les agents de serveur.

Connexion à un serveur Db2 distant

Par défaut, le serveur Db2 (Db2 Advanced Enterprise Server Edition version 10.5 groupe de correctifs 6) est installé en local avec le serveur Cloud APM. Si vous exécutez déjà Db2 Advanced Enterprise Server Edition version 10.5 groupe de correctifs 6 ou 9 ou Db2 Advanced Workgroup Server Edition V11.1.2, groupe de correctifs 2b ou V11.1.3, groupe de correctifs 3 sur un système externe, vous pouvez décider d'utiliser ce serveur Db2 distant pour les bases de données requises par le serveur Cloud APM au lieu d'installer le serveur Db2 local par défaut.

Avant de commencer

- Vérifiez que le système géré sur lequel est installé votre serveur Db2 distant exécute l'une des versions suivantes :
  - Db2 Advanced Enterprise Server Edition version 10.5, groupe de correctifs 6
  - Db2 Advanced Enterprise Server Edition version 10.5, groupe de correctifs 9
  - Db2 Advanced Workgroup Server Edition version 11.1.2, groupe de correctifs 2b
  - Db2 Advanced Workgroup Server Edition version 11.1.3, groupe de correctifs 3

  Si vous prévoyez d'utiliser Db2 Advanced Enterprise Server Edition V10.5, groupe de correctifs 9 ou Db2 Advanced Workgroup Server Edition V11.1.2, groupe de correctifs 2b ou V11.1.3, groupe de correctifs 3, veillez à installer le correctif temporaire 4 ou ultérieur d'IBM Cloud Application Performance Management Private, V8.1.4.0 après avoir terminé l'installation du serveur Cloud APM. Les correctifs temporaires pour le serveur Cloud APM version 8.1.4 peuvent être téléchargés à partir d'IBM Fix Central.
- Vérifiez que votre serveur Db2 distant exécute Red Hat Enterprise Linux version 6.* ou 7.* ou AIX version 7.1 ou 7.2.
- Pour plus d'informations sur le dimensionnement de vos serveurs, voir Chapitre 4, «Configuration requise», à la page 71. Ces informations permettent d'estimer la quantité d'entrée-sortie de disque escomptée en fonction de la taille de votre environnement. Une connexion réseau à faible temps d'attente entre le serveur Cloud APM et le serveur Db2 distant est également nécessaire. Veillez à maintenir le temps de réponse de la commande PING à 1 ms ou moins.
- Le programme d'installation de Db2 crée l'utilisateur dasuser1 et le groupe dasadm1, puis affecte l'utilisateur dasuser1 au groupe dasadm1. Vous devez créer manuellement tous les autres utilisateurs et groupes et affecter les utilisateurs aux groupes appropriés.
- Si vous utilisez un programme d'analyse antivirus (comme McAfee Virus Scan for Linux or Sophos), vous devez le configurer pour exclure tous les fichiers de base de données Db2, y compris les groupes de stockage, les espaces de table et les pools de mémoire tampon. Configurez le programme d'analyse antivirus avant de créer les bases de données Cloud APM.
- Vérifiez que le service cron est en cours d'exécution sur le serveur Db2. Le service cron est utilisé pour planifier les travaux d'élagage et d'agrégation de la base de données Datamart.
- La configuration `authentication=server` est l'authentification par défaut de l'installation Cloud APM lorsque les bases de données Db2 distantes sont cataloguées et qu'une base de données Db2 est créée. Vous pouvez utiliser `authentication=server_encrypt` si vous le souhaitez ou si vos règles de sécurité l'exigent. Pour plus d'informations, voir «Modification de l'authentification Db2 de server à server_encrypt», à la page 136.

Pourquoi et quand exécuter cette tâche

Ces étapes sont exécutées sur deux systèmes : le système sur lequel vous installez le serveur Cloud APM et un système externe sur lequel le serveur Db2 distant est installé.

IBM Data Server Client est installé sur le même système que le serveur Cloud APM. Il gère les applications sur les bases de données Db2 existantes sur le serveur Cloud APM. Les bases de données DATAMART, SCR32 et WAREHOUS sont créées sur le système externe. Ces bases de données sont requises par le serveur Cloud APM. En général, elles sont créées au cours de l'installation du serveur Cloud APM si le serveur Db2 local par défaut est installé. Vous devez toutefois les créer lors de la connexion à un serveur Db2 distant sur un système externe. Vous pouvez spécifier des noms personnalisés pour ces bases de données lors de l'utilisation d'un serveur Db2 distant.

Procédure

Pour configurer un serveur Db2 externe pour les bases de données du serveur Cloud APM, procédez comme suit :

1. Sur le système sur lequel vous installez le serveur Cloud APM, copiez les scripts de base de données de l'image d'installation du serveur Cloud APM sur le système externe :
   a. Téléchargez l'image d'installation du serveur Cloud APM. Pour plus d'informations, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
   b. Extrayez les fichiers d'installation du serveur comme indiqué à l'étape 3 de «Téléchargement et installation du serveur», à la page 141.
   c. Copiez les scripts suivants sur le système externe. Vérifiez que l'utilisateur *instance_db2_externe* a accès au répertoire du serveur serveur Db2 distant sur le système externe sur lequel sont copiés les fichiers SQL. *instance_db2_externe* est le nom de l'utilisateur d'instance du serveur Db2. Indiquez un nom d'utilisateur ou acceptez le nom d'utilisateur par défaut, qui est `db2apm`.

      Linux

      ```
      /support_installation/files/sql/create/create_tdw_db.sql
      /support_installation/files/sql/create/create_scr_db.sql
      /support_installation/files/sql/create/create_datamart_db.sql
      /support_installation/files/sql/update/update_tdw_performance.sql
      /support_installation/packages/SCR/setup-dbconfig-linux_64.bin
      ```

      AIX

      ```
      /support_installation/files/sql/create/create_tdw_db.sql
      /support_installation/files/sql/create/create_scr_db.sql
      /support_installation/files/sql/create/create_datamart_db.sql
      /support_installation/files/sql/update/update_tdw_performance.sql
      /support_installation/packages/SCR/setup-dbconfig-aix_64.bin
      ```

      où *support_installation* correspond au répertoire contenant les fichiers d'installation du serveur Cloud APM.

   Ces scripts sont utilisés plus tard dans cette procédure pour créer les bases de données DATAMART, SCR32 et WAREHOUS sur le système externe.
2. Sur le système externe, créez les bases de données et installez le serveur Db2 distant :
   a. Recherchez le chemin d'installation du serveur Db2 et vérifiez la version de Db2 installée :
      ```
      db2ls
      ```
   b. Vérifiez que la licence Db2 est installée :
      ```
      rép_install_Db2/Db2_version/adm/db2licm -l
      ```

      où *rép_install_Db2* est le chemin d'installation de Db2 que vous avez extrait à l'étape 2.a.
   c. Créez l'utilisateur *instance_db2_externe*, ajoutez-le au groupe db2iadm1 et créez l'instance de base de données : Linux

```
useradd -g db2iadm1 -m instance_db2_externe
/rép_install_Db2/version_Db2/instance/db2icrt -u db2fenc1
 instance_db2_externe
```

AIX

```
mkuser id=valeur pgrp=db2iadm1 groups=db2iadm1
home=/home/instance_db2_externe instance_db2_externe
chown -R instance_db2_externe:db2iadm1 /home/instance_db2_externe
/rép_install_Db2/version_Db2/instance/db2icrt -u db2fenc1
 instance_db2_externe
```

où AIX *valeur* est l'ID utilisateur. En général, 1000 et 1001 sont utilisés. Vous pouvez vérifier la disponibilité de ces ID dans SMIT : **smitty** > **Sécurité et utilisateurs** > **Utilisateurs** > **Répertorier tous les utilisateurs**. *version_Db2* est la version de Db2 installée. *version_Db2* peut ne pas être inclus dans le chemin lorsque vous installez vous-même le serveur Db2. Pour plus d'informations, voir «Utilisateurs et mots de passe par défaut», à la page 1075.

d. Créez l'utilisateur `itmuser`. Ajoutez l'utilisateur `itmuser` au groupe dasadm1 (applicable uniquement si vous exécutez Db2 version 10.5 groupe de correctifs 6 ou 9). Exécutez l'un des ensembles de commandes suivants en fonction de la version de Db2 que vous exécutez :
   - Pour Db2 version 10.5 groupe de correctifs 6 ou 9, exécutez les commandes suivantes :

     Linux

     ```
     useradd -g dasadm1 -m itmuser
     ```

     AIX

     ```
     mkuser id=valeur pgrp=dasadm1 groups=dasadm1 home=/home/itmuser itmuser
     ```

     AIX

     ```
     chown -R itmuser:dasadm1 /home/itmuser
     ```

     AIX où *valeur* est l'ID utilisateur.
   - Pour Db2 version 11.1.2 groupe de correctifs 2b ou version 11.1.3 groupe de correctifs 3, lancez les commandes suivantes :

     Linux

     ```
     useradd -m itmuser
     ```

     AIX

     ```
     mkuser id=valeur home=/home/itmuser itmuser
     ```

     AIX

     ```
     chown -R /home/itmuser
     ```

     AIX où *valeur* est l'ID utilisateur.

e. En tant que superutilisateur, définissez les mots de passe pour l'utilisateur *instance_db2_externe* et les comptes `itmuser` :

   ```
   passwd instance_db2_externe
   passwd itmuser
   ```

   Enregistrez les mots de passe quelque part car vous avez besoin de ces valeurs lorsque vous démarrez l'installation du serveur Cloud APM.

f. Dans un éditeur de texte, ouvrez le fichier `/etc/services`, puis ajoutez un nom de service et le numéro de port pour l'instance utilisateur *instance_db2_externe*. Par exemple :

   ```
   db2c_instance_db2_externe numéro_port/tcp
   ```

où *numéro_port* est le numéro de port que l'instance *instance_db2_externe* doit écouter. Enregistrez les valeurs de numéro de port quelque part car vous en aurez besoin lorsque vous démarrerez l'installation du serveur Cloud APM.

g. Configurez l'environnement de l'instance db2apm en entrant la commande suivante :

```
. /home/db2apm/sqllib/db2profile
```

h. Connectez-vous au compte utilisateur *instance_db2_externe*. Par exemple :

```
su - db2apm
```

i. Mettez à jour la configuration de Db2 avec le nom de service en entrant les commandes suivantes :

```
db2 update database manager configuration using svcename
 db2c_instance_db2_externe
db2stop
db2start
```

j. Si vous prévoyez d'utiliser l'authentification LDAP transparente sur le système sur lequel vous installez le serveur Cloud APM, définissez la variable de registre divers DB2AUTH sur OSAUTHDB dans l'instance Db2 :

```
db2set DB2AUTH=OSAUTHDB
db2stop
db2start
```

L'authentification LDAP transparente permet à l'instance Db2 d'authentifier les utilisateurs et d'accéder à leurs groupes par le biais du système d'exploitation. Le système d'exploitation, à son tour, effectue l'authentification au moyen d'un serveur LDAP.

k. Activez les communications TCP/IP :

```
db2set DB2COMM=tcpip
db2stop
db2start
```

l. Vérifiez que les bases de données WAREHOUS, SCR32 et DATAMART n'existent pas :

```
db2 list db directory
```

Si l'une des bases de données existe, supprimez-la à l'aide de la commande suivante :

```
db2 drop db nom_base_de_données
```

où *nom_base_de_données* est le nom de la base de données.

m. Suivez les étapes facultatives ci-dessous :

1) Pour que les bases de données Cloud APM utilisent un autre chemin que le chemin par défaut pour la base de données, ou pour modifier les noms de base de données par défaut, éditez les fichiers `create_tdw_db.sql`, `create_scr_db.sql` et `create_datamart_db.sql` pour spécifier les modifications avant de démarrer les scripts SQL pour créer les bases de données (étape suivante 2n, à la page 133). Par exemple, pour utiliser le chemin de base de données `/data/serveurapm1` pour les trois bases de données pour un serveur Cloud APM appelé serveurapm1, éditez les fichiers SQL pour inclure le nouveau chemin en ajoutant **ON** */data/serveurapm1*:

```
CREATE DATABASE DATAMART on /data/serveurapm1 USING CODESET UTF8 TERRITORY US
PAGESIZE 8 K
CREATE DATABASE SCR32 AUTOMATIC STORAGE YES on /data/serveurapm1 USING CODESET
UTF-8 TERRITORY US COLLATE USING SYSTEM PAGESIZE 8192
CREATE DATABASE WAREHOUS AUTOMATIC STORAGE YES on /data/serveurapm1
USING CODESET UTF-8 TERRITORY US COLLATE USING SYSTEM PAGESIZE 8192
```

Si vous avez mis à jour le chemin de répertoire, vérifiez qu'il est détenu par l'ID d'instance et qu'il est accessible en écriture pour ce dernier.

2) Utilisez un éditeur tel que vi, pour modifier les noms de la base de données dans les fichiers `create_tdw_db.sql` `create_scr_db.sql` et `create_datamart_db.sql`. Si vous modifiez le nom de la base de données *WAREHOUS*, le fichier `/installation_media/files/sql/update/update_tdw_performance.sql` est également affecté.

n. Créez les bases de données DATAMART, SCR32 et WAREHOUS en démarrant les scripts suivants :

```
db2 -vf /chemin/create_tdw_db.sql
db2 -vf /chemin/create_scr_db.sql
db2 -vf /chemin/create_datamart_db.sql
db2 -vf /chemin/update_tdw_performance.sql
```

où *chemin* correspond au chemin d'accès et au répertoire dans lequel vous avez stocké le script après l'avoir copié depuis le serveur Cloud APM. Ces scripts créent les bases de données dans le répertoire de base de l'utilisateur *instance_db2_externe*.

o. S'il s'agit de la première base de données SCR Cloud APM que vous avez créée pour l'instance Db2 instance, exécutez le script `setup-dbconfig-operating_system_64.bin` pour effectuer les étapes requises pour la base de données SCR32. Si vous avez déjà exécuté `setup-dbconfig-operating_system_64.bin.script` pour cette instance Db2, ignorez cette étape et suivez plutôt l'étape 2q, à la page 134.

```
/chemin/setup-dbconfig-système_d'exploitation_64.bin -i console
```

où *système_d'exploitation* est `aix` ou `linux`. Suivez les invites de la console :

1) A l'invite de sélection d'un environnement local, entrez `2` pour sélectionner l'anglais.
2) Entrez `1` pour accepter le contrat de licence.
3) Entrez le chemin d'accès absolu au répertoire d'installation. Le programme exécutable `setup-dbconfig` installe un programme utilisé pour la création de la base de données SCR dans ce répertoire. Il est utile de spécifier un répertoire sous votre répertoire de base. Par exemple, si l'instance Db2 est `db2apm` et que l'utilisateur **db2apm** exécute le programme `setup-dbconfig`, spécifiez le chemin suivant : `/home/db2apm/tbsmdb`. Le programme requiert environ 170 Mo d'espace disque.

   Pour accepter le chemin par défaut, appuyez sur la touche **Entrée**. Le chemin par défaut est `/opt/IBM/tivoli/tbsmdb`. Si vous acceptez ce chemin, avant de continuer l'installation, vérifiez que l'utilisateur d'instance Db2 dispose des droits nécessaires pour créer un répertoire dans `/opt/IBM` ou que le répertoire `/opt/IBM/tivoli/tbsmdb` existe déjà et que l'utilisateur d'instance DB2 y a accès en écriture.

   Si vous prévoyez d'installer plusieurs bases de données SCR32 sur ce serveur Db2 distant, utilisez un chemin unique pour chaque instance Db2. Par exemple, si le nom de l'instance Db2 est *db2apmg*, utilisez le chemin `/home/db2apmg/tbsmdb`. Le chemin n'est pas utilisé pour la base de données scr.
4) Entrez `1` pour sélectionner `IBM Cloud Application Performance Management (APM)` comme produit utilisant la base de données.
5) Entrez `1` pour sélectionner `Simple` comme type d'installation à exécuter.
6) Entrez `1` pour que le programme d'installation crée le schéma de base de données, notamment les tables, les espaces table et les vues.
7) Entrez les détails de configuration de la base de données suivants lorsque vous y êtes invité :

```
Nom de la base de données (8 caractères au maximum) (VALEUR PAR DEFAUT : SCR32): scr-database-name
Nom d'hôte ou adresse IP de la base de données (VALEUR PAR DEFAUT) : nom_hôte_ou_adresse_IP
Port (VALEUR PAR DEFAUT : 50000) : port
ID utilisateur de la base de données : ID_utilisateur_base_de_données
Mot de passe de la base de données : mot_de_passe_base_de_données
Confirmation du mot de passe : mot_de_passe_base_de_données
Chemin de la base de données (Valeur par défaut : <valeur par défaut>) :  chemin_par_défaut
```

Où :

nom_basededonnées_scr
Nom de la base de données SCR dans le fichier `create_scr_db.sql` que vous avez utilisé à l'étape 2n, à la page 133. Par défaut, il s'agit de *SCR32*.

port Numéro de port indiqué à l'étape 2e.

ID_utilisateur_base_de_données
L'ID utilisateur est généralement `itmuser`, bien que l'ID utilisateur *instance_db2_externe* puisse être utilisé.

chemin_par_défaut
Système de fichiers où la base de données est écrite. La valeur par défaut est le répertoire de base de l'utilisateur. Si, à l'étape 2k, vous avez indiqué un autre chemin dans les scripts, vous devez impérativement indiquer le même système de fichiers dans le *chemin_par_défaut*.

Remarque : Si le nom par défaut n'est pas utilisé à l'étape 2m, à la page 132, mettez à jour le nom de la base de données.

8) A l'invite `L'utilisateur spécifié dispose-t-il de l'autorité SYSCTRL ou SYSADM ?`, entrez `2 "Non"` si `itmuser` a été spécifié ou `1 "Oui"` si l'utilisateur *instance_db2_externe* a été spécifié.
9) Entrez `2` pour indiquer de ne pas chiffrer la base de données.
10) Si l'utilisateur de base de données que vous avez spécifié ne dispose pas de l'autorité SYSCTRL ou SYSADM, entrez-en un qui dispose de cette autorité. Indiquez le nom d'utilisateur *instance_db2_externe*.

Remarque : Passez à l'étape 2r, à la page 135.

p. Entrez la commande suivante afin d'activer le planificateur DB2 que Datamart utilise pour l'agrégation et l'élagage.

```
db2set DB2_ATS_ENABLE=YES
```

Pour plus d'informations, voir la rubrique db2set - DB2 profile registry command dans l'IBM Knowledge Center de DB2.

q. Exécutez le script `setup-dbconfig-operating_system_64.bin` une seule fois pour chaque instance Db2. Si vous avez déjà exécuté le script `setup-dbconfig-operating_system_64.bin` pour cette instance Db2, lors de la création d'une base de données SCR pour un autre serveur Cloud APM, procédez comme suit :

1) Accédez au répertoire que vous avez entré à l'étape 2o3, à la page 133 pour l'utilisateur d'instance Db2, par exemple :

```
cd /home/db2apmg/tbsmdb
```

2) Exécutez les commandes **grep** suivantes :

```
grep "DL_DBManager.ObjectURL="
tools/XMLtoolkit/bin/xmltoolkitsvc.properties
grep "TBSM.UDF.DatabaseName="  sql/tbsmudf_db.properties
grep "TBSM.DatabaseName="      sql/tbsm_db.properties
grep "TBSM.OnPath="            sql/tbsm_db.properties
grep "TBSM.Port="              sql/tbsm_db.properties
```

La sortie suivante s'affiche :

```
[db2apmg@db21056 ~]$ cd /home/db2apmg/tbsmdb
[db2apmg@db21056 tbsmdb]$ grep "DL_DBManager.ObjectURL="
tools/XMLtoolkit/bin/xmltoolkitsvc.properties
DL_DBManager.ObjectURL=jdbc:db2://db21056.rtp.raleigh.ibm.com:50005/SCgmmg
[db2apmg@db21056 tbsmdb]$ grep "TBSM.UDF.DatabaseName="  sql/tbsmudf_db.properties
TBSM.UDF.DatabaseName=SCgmmg
[db2apmg@db21056 tbsmdb]$ grep "TBSM.DatabaseName="      sql/tbsm_db.properties
TBSM.DatabaseName=SCgmmg
```

```
[db2apmg@db21056 tbsmdb]$ grep "TBSM.OnPath="           sql/tbsm_db.properties
TBSM.OnPath= ON /db2/SCgmmg_data
[db2apmg@db21056 tbsmdb]$ grep "TBSM.Port="             sql/tbsm_db.properties
TBSM.Port=50005
```

3) Mettez à jour les fichiers pour qu'ils correspondent au port et au nom de la base de données SCR.

4) Utilisez la commande **tbsm_db.sh** pour créer des tables et des vues associées à la base de données :

```
./bin/tbsm_db.sh -s sc -U dbUserId -f c
```

où : *dbUserid* est l'utilisateur d'instance Db2. Les pools de mémoire tampon et les espaces table sont également créés.

r. Entrez la commande suivante en tant qu'utilisateur *instance_db2_externe* pour chaque base de données afin d'ajuster le pool de mémoire tampon et le journal des transactions, après avoir déterminé la taille de votre environnement.

```
db2 connect to WAREHOUS
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size NBR_PAGES_WAREHOUS
db2 disconnect WAREHOUS
db2 connect to DATAMART
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size NBR_PAGES_DATAMART
db2 disconnect DATAMART
db2 connect to SCR32
db2 UPDATE DATABASE CONFIGURATION FOR SCR32 USING LOGSECOND 25
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size 5000
db2 alter bufferpool TBSMCFG16KBP IMMEDIATE size 10000
db2 alter bufferpool TBSM4KBP IMMEDIATE size 1000
db2 alter bufferpool TBSM32KBP IMMEDIATE size 1000
db2 alter bufferpool TBSMSCR16KBP IMMEDIATE size NBR_PAGES_SCR32
db2 disconnect SCR32
```

Où :

WAREHOUS_PAGE_COUNT
Nombre de pages de pool de mémoire tampon (pages de 8 K) : 75000 pour Petite ; 100000 pour Moyenne ou 100000 pour Grande.

NBR_PAGES_DATAMART
Nombre de pages de pool de mémoire tampon (pages de 8 K) : 100000 pour Petite ; 200000 pour Moyenne ou 300000 pour Grande.

NBR_PAGES_SCR32
Nombre de pages de pool de mémoire tampon (pages de 16 K) : 15000 pour Petite, 30000 pour Moyenne et 30000 pour Grande.

Estimez la taille de votre environnement (Petite, Moyenne ou Grande) d'après le tableau de la configuration requise pour le serveur Cloud APM dans «Configuration matérielle requise pour le serveur Cloud APM», à la page 92.

Remarque : Si vous n'utilisez pas les noms de base de données par défaut, remplacez les noms *WAREHOUS*, *DATAMART* et *SCR32* par ceux que vous avez utilisés à l'étape 2m, à la page 132.

s. Si vous voulez exécuter le serveur avec l'authentification Db2 définie sur **server_encrypt**, effectuez les étapes 1, à la page 137 à 2, à la page 137 de la rubrique *Modification de l'authentification Db2 de server à server_encrypt*.

3. En tant que superutilisateur, installez IBM Data Server Client sur le système où vous prévoyez d'installer le serveur Cloud APM (la version de Data Server Client doit correspondre à celle du serveur Db2 mentionné dans la section Avant de commencer).

Le client IBM Data Server nécessite que l'utilisateur local Db2 du serveur Cloud APM exécute des commandes Db2. Ce nom d'utilisateur local Db2 a toujours pour valeur `db2apm`. Ne confondez pas cet utilisateur `db2apm` avec l'utilisateur *instance_db2_externe* distant créé au cours des étapes précédentes.

a. Créez l'utilisateur db2apm et ajoutez-le au groupe db2iadm1 :
```
groupadd db2iadm1
useradd -g db2iadm1 -m db2apm
```
b. Créez l'utilisateur db2fenc1 et ajoutez-le au groupe db2fadm1 :
```
groupadd db2fadm1
useradd -g db2fadm1 -m db2fenc1
```
c. Installez le composant IBM Data Server Client à partir du module d'installation Db2 qui se trouve dans l'image d'installation du serveur Cloud APM : packages/DB2/v10.5fp6_linuxx64_server_t.tar.gz. Extrayez le module à l'aide de tar -xzvf v10.5fp6_linuxx64_server_t.tar.gz et accédez au répertoire server_t. Si vous utilisez la version locale du serveur Db2 installé avec le serveur Cloud APM, assurez-vous que la version de Data Server Client correspond à celle du serveur Db2. Si vous utilisez un serveur Db2 distant, assurez-vous que la version de Data Server Client correspond à celle du serveur Db2 distant. Consultez les versions du serveur Db2 local et distant dans la section Avant de commencer.

   Remarque : Assurez-vous que la version de Data Server Client correspond à la version du serveur Db2 distant.
d. Démarrez le script db2setup :
```
./db2setup
```

   Pour exécuter le script db2setup, vous devez définir la variable d'environnement *DISPLAY* pour établir une connexion à un serveur X11.
e. Après que le tableau de bord Db2 s'ouvre, sélectionnez **Install a Product**, puis sélectionnez le client que vous voulez installer et suivez les invites dans l'assistant de configuration Db2.
f. Acceptez le contrat de licence.
g. Définissez le type d'installation sur **Typical**.
h. Dans la fenêtre de configuration d'une instance Db2, sélectionnez **Create a DB2 instance**.
i. Cliquez sur **Existing User** et entrez db2apm pour le nom d'utilisateur. Vous pouvez également entrer la commande suivante à partir d'une ligne de commande une fois l'installation terminée :
```
/opt/ibm/db2/version_Db2/instance/db2icrt -u db2fenc1 db2apm
```

   où *version_Db2* est la version de Db2 installée.
j. Cliquez sur **Suivant**, puis sur **Terminer**.

Que faire ensuite

Installez l'serveur Cloud APM. Commencez à l'étape 4, à la page 142 dans «Téléchargement et installation du serveur», à la page 141.

Tâches associées:

«Modification des mots de passe sur un serveur Db2 distant», à la page 1077
Si votre serveur Cloud APM utilise un serveur Db2 distant sur un système externe, suivez cette procédure pour changer les mots de passe des utilisateurs Db2 sur le serveur Db2 et configurer le serveur Cloud APM avec le mot de passe itmuser mis à jour. Ces étapes diffèrent légèrement de la procédure de modification des mots de passe de l'utilisateur Db2 sur le serveur Cloud APM connecté au serveur Db2 local par défaut.

Modification de l'authentification Db2 de server à server_encrypt

En raison des règles de sécurité de l'entreprise, il se peut que vous ne puissiez pas ou ne vouliez pas utiliser la configuration authentication=server dans le cadre de l'authentification Db2. Lorsque vous créez une base de données Db2 distante ou que vous basculez de la base de données Cloud APM Db2 locale vers un serveur Db2 distant, vous pouvez redéfinir l'authentification sur authentication=server_encrypt afin de protéger vos ID utilisateur et mot de passe.

Pourquoi et quand exécuter cette tâche

La configuration `authentication=server` est l'authentification par défaut de l'installation Cloud APM lorsque les bases de données Db2 distantes sont cataloguées et qu'une base de données Db2 est créée. La procédure consiste à mettre à jour la configuration de l'authentification Db2 sur `server_encrypt` et d'éditer le fichier `install.properties` situé dans le module d'installation du serveur Cloud APM.

Procédure

Effectuez les étapes suivantes sur le serveur Db2 distant en tant qu'utilisateur d'instance Db2 (`db2apm` est l'utilisateur d'instance dans les commandes) :

1. Vérifiez la configuration de l'authentification Db2 :
   a. `db2 attach to db2apm`
   b. `db2 get dbm cfg | grep AUTHENTICATION`

      La commande grep imprime `Database manager authentication (AUTHENTICATION) = SERVER`. Si, au lieu de cela, vous obtenez `Database manager authentication (AUTHENTICATION) = SERVER_ENCRYPT`, vous pouvez ignorer l'étape 2.
   c. `db2 attach to db2apm`
   d. `db2 detach`
2. Redéfinissez l'authentification Db2 sur server_encrypt :
   a. `db2 attach to db2apm`
   b. `db2 update dbm cfg using authentication server_encrypt`
   c. `db2 get dbm cfg | grep AUTHENTICATION`

      La commande grep imprime `Database manager authentication (AUTHENTICATION) = SERVER_ENCRYPT`.
   d. `db2 attach to db2apm`
   e. `db2 detach`

Résultats

L'authentification d'utilisateur au serveur de base de données est désormais définie sur `server_encrypt`.

Tâches associées:

«Connexion à un serveur Db2 distant», à la page 129
Par défaut, le serveur Db2 (Db2 Advanced Enterprise Server Edition version 10.5 groupe de correctifs 6) est installé en local avec le serveur Cloud APM. Si vous exécutez déjà Db2 Advanced Enterprise Server Edition version 10.5 groupe de correctifs 6 ou 9 ou Db2 Advanced Workgroup Server Edition V11.1.2, groupe de correctifs 2b ou V11.1.3, groupe de correctifs 3 sur un système externe, vous pouvez décider d'utiliser ce serveur Db2 distant pour les bases de données requises par le serveur Cloud APM au lieu d'installer le serveur Db2 local par défaut.

«Déplacement des bases de données Db2 vers un autre serveur Db2 ou une instance Db2 différente», à la page 1079
Après avoir installé le serveur Cloud APM, vous pouvez déplacer les bases de données Db2 du serveur Cloud APM local vers un serveur Db2 distant ou si vous êtes déjà connecté à un serveur Db2 distant, vous pouvez déplacer les bases de données vers un autre serveur Db2 distant ou vers un utilisateur d'instance Db2 différent.

Passage d'une offre à une autre

Dans la version 8.1.4, faisant suite à une nouvelle stratégie de marque, deux offres sont prises en charge, au lieu de quatre comme dans la version 8.1.3. Ces offres sont IBM Cloud Application Performance Management, Base Private et IBM Cloud Application Performance Management, Advanced Private. Vous pouvez passer de l'offre Cloud APM, Base à l'offre Cloud APM, Advanced à tout moment après avoir installé l'offre Cloud APM, Base ou effectué une mise à niveau vers l'offre Cloud APM, Base.

Pourquoi et quand exécuter cette tâche

Lorsque vous démarrez le script d'installation, vous recevez un rapport vous indiquant l'offre actuellement installée, ainsi que l'offre qui sera installée une fois la procédure terminée. Le passage de Cloud APM, Base à Cloud APM, Advanced peut prendre plus de temps que l'installation de Cloud APM, Advanced uniquement car différents composants sont arrêtés et démarrés pour remplacer Cloud APM, Base par Cloud APM, Advanced. L'offre Cloud APM, Advanced remplace l'offre Cloud APM, Base. L'offre finale installée est Cloud APM, Advanced.

Procédure

Pour passer de l'offre Cloud APM, Base à l'offre Cloud APM, Advanced, procédez comme suit :

Téléchargez et installez l'offre Cloud APM, Advanced. Pour plus d'informations, voir «Téléchargement et installation du serveur», à la page 141.

Résultats

L'offre Cloud APM, Advanced est installée en remplaçant l'offre Cloud APM, Base existante.

Que faire ensuite

Pour utiliser les fonctionnalités de l'Agent WebSphere Applications fournies dans la nouvelle offre, vous devez reconfigurer le collecteur de données. Pour obtenir des instructions, voir «Reconfiguration du collecteur de données en cas de modification du type d'offre sur le serveur Cloud APM», à la page 799.

Installation sur un système à l'aide d'un service d'annuaire externe

Si le système sur lequel vous prévoyez d'installer le serveur Cloud APM avec un serveur Db2 local utilise un service d'annuaire LDAP externe pour authentifier les utilisateurs qui se connectent au serveur Cloud APM, tels que votre superutilisateur et vos utilisateurs Db2, vous devez créer des utilisateurs Db2 locaux avant d'installer le serveur Cloud APM.

Avant de commencer

Bien que cette procédure s'applique généralement à n'importe quel service d'annuaire et protocole d'accès, les étapes suivantes s'appliquent à un service d'annuaire externe utilisé avec LDAP. Il est possible que le service d'annuaire et le protocole d'accès que vous avez choisis ne soient pas reconnus par Db2 et par le logiciel d'installation du serveur Cloud APM. Dans un tel scénario, lorsque vous tentez de gérer des ressources dans ce service d'annuaire, une erreur est renvoyée car vous n'êtes pas autorisé à terminer ces tâches. Les étapes qui diffèrent en fonction du type de service d'annuaire sont signalées dans cette procédure mais ne sont pas documentées.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour :

- Désactivez temporairement l'authentification LDAP pour le serveur Cloud APM.

- Créez des utilisateurs et des groupes Db2 locaux.
- Configurez les utilisateurs et les mots de passe Db2 dans le fichier `install.properties` utilisé pour l'installation du serveur Cloud APM.
- Réactivez l'authentification LDAP.
- Installez l'serveur Cloud APM.
- Configurez le plug-in de sécurité LDAP sur le serveur Db2 local.
- Mettez à jour les mots de passe de l'utilisateur itmuser et de l'utilisateur de l'instance Db2 si ceux-ci sont configurés dans votre service d'annuaire externe utilisé avec LDAP.
- Installez un serveur Db2 local à utiliser avec LDAP pour l'authentification des utilisateurs.

Remarque : L'installation du serveur Cloud APM ne configure pas le serveur Db2 local pour l'utilisation du plug-in de sécurité LDAP. Après avoir installé le serveur Cloud APM, vous devez configurer le plug-in de sécurité LDAP sur le serveur Db2 local.

Procédure

1. Entrez la commande suivante et sauvegardez la sortie pour référence ultérieure :

   ```
   id nom_utilisateur
   ```

   où *nom_utilisateur* est `itmuser`, `db2apm`, `db2fenc1` ou `dasusr1`. Exemple de sortie :

   ```
   # id itmuser
   uid=1188800003(itmuser) gid=1188800003(itmuser) groups=1188800003(itmuser)
   # id db2apm
   uid=1188800004(db2apm) gid=1188800004(db2apm) groups=1188800004(db2apm)
   # id db2fenc1
   uid=1188800005(db2fenc1) gid=1188800005(db2fenc1) groups=1188800005(db2fenc1)
   # id dasusr1
   uid=1188800006(dasusr1) gid=1188800006(dasusr1) groups=1188800006(dasusr1)
   ```

   Important : Le message `id: <nom_utilisateur>: No such user` indique que l'utilisateur n'est pas défini dans l'annuaire LDAP. Si aucun des utilisateurs n'est défini dans l'annuaire LDAP, ignorez les étapes restantes. Si un sous-ensemble des autres utilisateurs est défini dans l'annuaire LDAP, n'effectuez les étapes restantes que pour les utilisateurs qui se trouvent dans l'annuaire LDAP.
2. Désactivez le service d'authentification LDAP en entrant la commande suivante :

   ```
   service sssd stop
   ```

   La commande à exécuter pour cette étape peut différer en fonction du service d'annuaire choisi.
3. Effectuez un nettoyage du cache SSSD pour les utilisateurs que vous avez identifiés à l'étape 1. Par exemple :

   ```
   sss_cache -u itmuser
   sss_cache -u db2apm
   sss_cache -u db2fenc1
   sss_cache -u dasusr1
   ```

   Cette étape peut différer en fonction du service d'annuaire choisi.
4. Créez des groupes et des utilisateurs sur votre système local pour les utilisateurs que vous avez identifiés à l'étape 1. Réutilisez les noms de groupe et ID de groupe, ainsi que les noms d'utilisateur et ID d'utilisateur indiqués dans la sortie de la commande `id` à l'étape 1. Utilisez les mots de passe spécifiés dans l'annuaire LDAP.

   ```
   groupadd -g 1188800003 itmuser
   useradd -u 1188800003 -g 1188800003 itmuser
   passwd itmuser

   groupadd -g 1188800004 db2apm
   useradd -u 1188800004 -g 1188800004 db2apm
   passwd db2apm
   ```

```
groupadd -g 1188800005 db2fenc1
useradd -u 1188800005 -g 1188800005 db2fenc1
passwd db2fenc1

groupadd -g 1188800006 dasusr1
useradd -u 1188800006 -g 1188800006 dasusr1
passwd dasusr1
```

5. Dans le fichier *image_install*/install.properties, mettez à jour les mots de passe des utilisateurs que vous avez identifiés à l'étape 1. Utilisez les mots de passe spécifiés dans l'annuaire LDAP. Par exemple :

   ```
   db2apm.password=db2Usrpasswd@08
   itmuser.password=db2Usrpasswd@08
   db2fenc1.password=db2Usrpasswd@08
   dasusr1.password=db2Usrpasswd@08
   ```

6. Dans le fichier image_install/files/db2wse.rsp, mettez à jour les noms de groupe des utilisateurs que vous avez identifiés à l'étape 1. Il n'existe aucune propriété pour l'utilisateur itmuser.
   a. Mettez à jour la propriété apm.GROUP_NAME avec le nom du groupe principal de l'utilisateur db2apm. Par exemple : apm.GROUP_NAME = db2apm
   b. Mettez à jour la propriété apm.FENCED_GROUP_NAME avec le nom du groupe principal de l'utilisateur db2fenc1. Par exemple : apm.FENCED_GROUP_NAME = db2fenc1
   c. Mettez à jour la propriété DAS_GROUP_NAME avec le nom du groupe principal de l'utilisateur dasusr1. Par exemple : DAS_GROUP_NAME = dasusr1
7. Activez le service d'authentification LDAP en entrant la commande suivante :

   ```
   service sssd start
   ```

   La commande à exécuter pour cette étape peut différer en fonction du service d'annuaire choisi.
8. Installez le serveur Cloud APM et sélectionnez l'option d'installation du serveur Db2 par défaut. Pour plus d'informations, voir «Téléchargement et installation du serveur», à la page 141.
9. Configurez le plug-in de sécurité LDAP sur le serveur Db2 local. Pour plus d'informations, voir LDAP-based authentication and group lookup support. Cette étape peut différer en fonction du service d'annuaire choisi.

Résultats

Le serveur Cloud APM est installé sur un système ou une machine virtuelle où LDAP est utilisé pour l'authentification d'utilisateur et où un serveur Db2 local est utilisé.

Que faire ensuite

Vérifiez que les données provenant de vos agents s'affichent dans la console Cloud APM. Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 989.

Création d'utilisateurs Db2 avant la connexion à un serveur Db2 local

Si vous prévoyez de vous connecter à un serveur Db2 local, vous pouvez créer les utilisateurs d'instance Db2 avant d'installer le serveur Cloud APM pour respecter les règles d'administration de serveur de base de données de votre organisation ou spécifier des mots de passe personnalisés. Vous devez affecter les utilisateurs Db2 à leur groupe principal lors de la création de chaque ID utilisateur.

Pourquoi et quand exécuter cette tâche

Lorsque vous avez choisi d'installer la base de données Db2 lors de l'installation du serveur Cloud APM, un serveur Db2 est créé avec les utilisateurs d'instance Db2 dasusr1, db2apm, db2fenc1 et itmuser ainsi que les groupes dasadm1, db2iadm1 et db2fadm1. L'installation affecte les utilisateurs aux groupes :

- L'utilisateur dasusr1 est affecté au groupe dasadm1
- L'utilisateur db2apm est affecté aux groupes db2iadm1 et dasadm1
- L'utilisateur db2fenc1 est affecté au groupe db2fadm1
- L'utilisateur itmuser est affecté au groupe dasadm1

Plutôt que de créer les utilisateurs et les groupes lors de l'installation du serveur, vous créez, grâce à ces instructions, les utilisateurs d'instance Db2 avant d'installer le serveur Cloud APM et le serveur Db2. Chaque fois que vous créez un utilisateur, vous devez l'affecter à son groupe principal et mettre à jour son mot de passe utilisateur par défaut dans le fichier `install.properties`. Il est également possible d'ajouter les utilisateurs à d'autres groupes utilisés dans votre environnement.

Procédure

En tant que superutilisateur, suivez les étapes ci-dessous :

1. Créez les groupes principaux. Par exemple,

   ```
   groupadd dasadm1
   groupadd db2iadm1
   groupadd db2fadm1
   ```

2. Créez les ID utilisateur et affectez chacun d'eux à un groupe principal. Par exemple,

   ```
   useradd -g dasadm1 -m dasusr1
   useradd -g db2iadm1 -m db2apm
   useradd -g db2fadm1 -m db2fenc1
   useradd -g dasadm1 -m itmuser
   ```

3. Définissez les mots de passe des ID utilisateur. Par exemple,

   ```
   passwd dasusr1
   passwd db2apm
   passwd db2fenc1
   passwd itmuser
   ```

4. Mettez à jour les mots de passe dans le fichier *image_installation_serveur_APM*/`install.properties` pour chaque utilisateur.

Que faire ensuite

Passez en revue les options et les exigences dans «Préparation de l'installation du serveur», à la page 125 afin de vous aider à planifier votre installation du serveur Cloud APM.

Téléchargement et installation du serveur

La procédure d'installation implique le téléchargement du support d'installation du serveur Cloud APM, l'extraction des fichiers d'installation sur le système et l'exécution du script d'installation.

Avant d'installer les agents de surveillance ou la Passerelle hybride ou de configurer les collecteurs de données, installez le serveur Cloud APM sur une machine virtuelle ou un ordinateur de votre réseau exécutant Red Hat Enterprise Linux.

Avant de commencer

Passez en revue les exigences et les options décrites dans «Préparation de l'installation du serveur», à la page 125.

Procédure

Alors que vous êtes connecté en tant que superutilisateur (dont les droits sont requis pour installer et exécuter le serveur Cloud APM), procédez comme suit pour télécharger, décompresser et installer le serveur et les composants de prise en charge sur un système Red Hat Enterprise Linux :

1. Téléchargez l'image d'installation du serveur Cloud APM à partir du site de téléchargement vers l'emplacement de transfert de votre choix. Voir «Téléchargement depuis Passport Advantage», à la page 118.
2. Si vous prévoyez de configurer les images d'agent et/ou l'image de la Passerelle hybride lors de l'installation du serveur, téléchargez les images sur le système sur lequel le serveur sera installé. Pour les détails, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Extrayez les fichiers d'installation du serveur pour votre offre :

   IBM Cloud Application Performance Management, Advanced Private
   `advanced_8.1.4.0.tar`

   IBM Cloud Application Performance Management, Base Private
   `base_8.1.4.0.tar`
4. Accédez au répertoire dans lequel vous avez extrait les fichiers d'installation du serveur.
5. Vérifiez que les droits par défaut sont définis correctement. Ouvrez une invite de commande et entrez `umask`.

   Une valeur de `0022` est renvoyée si les droits sont définis correctement. Si toute autre valeur est renvoyée, définissez les droits appropriés en entrant la commande suivante :

   ```
   umask 0022
   ```
6. Si vous souhaitez remplacer le protocole de communication HTTP par défaut par le protocole HTTPS (sécurisé), entrez la commande suivante :

   ```
   export APM_SECURE_COMMUNICATION=y
   ```

   (Voir «Définition des communications HTTP ou HTTPS», à la page 128.)
7. Si vous décidez d'utiliser une base de données Db2 distante plutôt que d'installer un serveur Db2 en local avec le serveur Cloud APM («Connexion à un serveur Db2 distant», à la page 129) et que vous avez créé les bases de données Cloud APM avec l'authentification Db2 définie sur `server_encrypt` et non sur la valeur `server` par défaut, procédez comme suit :
   a. Accédez au répertoire dans lequel vous avez décompressé le fichier tar d'installation du serveur Cloud APM.
   b. Editez le fichier `install.properties` de façon à définir `db2.authentication=server_encrypt`.
8. Si vous décidez d'utiliser une base de données Db2 distante au lieu d'installer un serveur Db2 en local avec le serveur Cloud APM et avez créé des bases de données ayant des noms personnalisés sur le serveur Db2 distant, procédez comme suit :
   a. Connectez-vous en tant qu'utilisateur db2apm sur le serveur Cloud APM.
   b. Si vous n'utilisez pas les noms de base de données par défaut, vous devez créer des entrées de catalogue d'alias pour que les noms par défaut fassent référence aux noms de vos bases de données. Cataloguez le noeud et les bases de données, par exemple :

      ```
      db2 CATALOG TCPIP NODE APM5 REMOTE 9.42.13.5 SERVER 50005
      ```

      où :
      - *APM5* est le nom du noeud. Utilisez n'importe quel nom (comportant jusqu'à 8 caractères) à l'exception de *APM_NODE* car ce dernier est utilisé par Cloud APM.
      - *9.42.13.5* est l'adresse IP ou le nom d'hôte du serveur Db2 distant.
      - *50005* est le numéro de port configuré pour l'instance Db2 sur le serveur Db2 distant.
   c. Si les entrées par défaut sont déjà cataloguées à partir d'une installation précédente, décataloguez les bases de données par défaut comme suit :

      ```
      db2 uncatalog db warehous
      db2 uncatalog db datamart
      db2 uncatalog db scr32
      ```
   d. Cataloguez les noms de vos bases de données en tant que nouveaux noms de base de données par défaut :

```
db2 CATALOG DB WHOUS5 as WAREHOUS at NODE APM5
db2 CATALOG DB DMART5 as DATAMART at NODE APM5
db2 CATALOG DB SCR5 as SCR32 at NODE APM5
```

où *WHOUS5* est votre nom pour la base de données WAREHOUS. *DMART5* est votre nom pour la base de données DATAMART. *SCR5* est votre nom pour la base de données SCR32. *APM5* est le noeud que vous avez créé à l'étape 8b, à la page 142.

Remarque : Si vous avez ajouté **db2.authentication=server_encrypt** au fichier `install.properties` à l'étape 7b, à la page 142, ajoutez **authentication server_encrypt** à chaque commande **db2 CATALOG**.

e. Testez la connexion à la base de données distante, par exemple :

```
db2 connect to  warehous user itmuser
db2 terminate
```

Une sortie semblable à la suivante s'affiche :

```
[db2apm@APM814c ~]$ db2 connect to warehous user itmuser
Enter current password for itmuser:

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = ITMUSER
 Local database alias   = WAREHOUS

[db2apm@APM814c ~]$ db2 terminate
DB20000I  The TERMINATE command completed successfully.
```

f. Connectez-vous en tant que superutilisateur sur le serveur Cloud APM.

g. Recherchez le fichier `install.properties` dans le package du média d'installation. Il se trouve dans le même répertoire que le script `install.sh`. Sauvegardez une copie de sauvegarde du fichier et éditez-la. Le fichier comporte trois lignes qui contiennent les noms des bases de données Cloud APM :

```
datamartdb.name=DATAMART
 metriccachedb.name=WAREHOUS
 topologydb.name=SCR32
```

Modifiez les noms pour qu'ils correspondent à ceux de vos bases de données et sauvegardez le fichier :

```
datamartdb.name=DMART5
 metriccachedb.name=WHOUS5
 topologydb.name=SCR5
```

9. Installez le serveur Cloud APM sur la machine virtuelle ou sur votre système informatique :

a. Entrez l'une des commandes suivantes pour exécuter le script d'installation :

- Installez le serveur dans le répertoire `/opt/ibm` par défaut :

  ```
  ./install.sh
  ```

- Installez le serveur dans le répertoire de votre choix :

  ```
  ./install.sh -d /custom/path/
  ```

  où */custom/path/* est le chemin d'accès au répertoire dans lequel vous voulez installer le serveur.

- Installez le serveur et affichez la sortie sur la console :

  ```
  ./install.sh -v
  ```

  La sortie est sauvegardée dans le fichier journal d'installation que vous choisissiez l'option prolixe (**-v**) ou non. Vous pouvez entrer les options de répertoire (**-d**) et prolixe (**-v**) dans la commande : `./install.sh -d -v`.

b. Lorsque vous êtes invité à effectuer la mise à niveau à partir d'une installation existante, entrez 2 (non). Le programme d'installation vérifie l'éventuelle offre déjà installée et l'offre que vous êtes en train d'installer, puis vous demande de confirmer que vous souhaitez continuer.

c. Passez en revue l'offre qui s'affiche et entrez 1 (oui) pour continuer l'installation ou 2 (non) pour arrêter l'installation.

d. Lorsque vous êtes invité à modifier le répertoire d'installation par défaut, entrez 1 pour spécifier un autre répertoire ou 2 pour accepter le répertoire `/opt/ibm` par défaut.

e. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser.

f. A l'invite de modification du mot de passe par défaut du compte administrateur, entrez 1 (oui) pour créer un nouveau mot de passe chiffré ou 2 (non) pour conserver le mot de passe par défaut non chiffré «apmpass». Si vous modifiez le mot de passe, conservez-en une copie en lieu sûr ; vous ne pourrez pas récupérer le mot de passe si vous l'oubliez. Une fois que vous avez répondu à l'invite de modification du mot de passe de l'administrateur, l'installation se poursuit.

g. Lorsque vous êtes invité à configurer les images d'installation des agents, du collecteur de données et de la Passerelle hybride (si cette dernière est utilisée) pour vous connecter au serveur, entrez 1 (oui) pour configurer les images maintenant ou 2 (non) pour reporter la configuration des images des agents, du collecteur de données et de la Passerelle hybride.

h. Si vous avez entré 1 (oui), vous êtes invité à confirmer les informations suivantes :
   - Le chemin d'accès au répertoire sur le serveur sur lequel sont stockées les images d'agent, du collecteur de données et de la Passerelle hybride (si cette dernière est utilisée).
     Les images d'agent, du collecteur de données et de la Passerelle hybride peuvent être montées sur une partition NFS, mais elles doivent être accessibles à l'aide du système de fichiers.
   - Modifier ou non le répertoire des images configurées (1 - oui) ou accepter le répertoire *rép_install*`/ccm/depot` par défaut (2 - non). Si vous avez sélectionné 1 (oui), entrez le répertoire des images configurées à stocker.
   - Si vous avez accepté le répertoire par défaut de stockage des images d'agent, du collecteur de données et de la Passerelle hybride configurées, le programme d'installation crée le répertoire *rép_install*`/ccm/depot` de stockage des images d'agent, du collecteur de données et de la Passerelle hybride configurées. Toutefois, si vous avez choisi de modifier le répertoire, si le programme d'installation ne parvient pas à créer ce répertoire ou que ce dernier n'est pas accessible en écriture, vous êtes invité à spécifier le répertoire de sortie.

   Si vous avez entré 2 (non), cette étape est ignorée.

i. Lorsque vous êtes invité à saisir l'adresse IP et le nom d'hôte que les agents utiliseront pour communiquer avec le serveur, entrez l'adresse IP ou le nom d'hôte du serveur pour les agents et la Passerelle hybride à utiliser. Le format de l'adresse IP peut être IPv4 ou correspondre au nom de domaine complet. Vous pouvez modifier l'adresse IP et le nom d'hôte ultérieurement. Voir «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.

j. Lorsque vous êtes invité à entrer les valeurs suivantes, entrez celles qui concernent le serveur utilisé dans un navigateur Web pour se connecter à la console Cloud APM. Cette valeur correspond à l'adresse que les utilisateurs entrent pour démarrer la console Cloud APM depuis leurs navigateurs Web.
   - Nom de domaine complet, par exemple : `myserver.example.com`.
   - Nom d'hôte abrégé
   - Adresse IP

   Conseil : Le nom de domaine complet et le nom d'hôte abrégé sont résolus à l'aide du DNS. Si votre système n'a pas la bonne résolution DNS, entrez l'adresse IP pour chacune des trois valeurs. Vous pouvez modifier l'adresse IP et le nom d'hôte ultérieurement. Voir «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.

k. Lorsque vous êtes invité à installer la base de données ou à vous connecter à une base de données Db2 existante, entrez 1 pour installer la base de données par défaut ou 2 pour vous connecter à une base de données Db2 existante.

   Si vous avez saisi 2 (se connecter à la base de données existante), procédez comme suit :

   - Une invite vous demande de fournir des valeurs ou d'accepter les valeurs par défaut pour les paramètres Db2 nom d'hôte/adresse IP et numéro de port, pour l'établissement de la connexion.
   - Saisissez le mot de passe pour l'utilisateur itmuser que vous avez créé lors de la configuration du système Db2 distant.
   - Saisissez le nom d'utilisateur distant *instance_db2_externe* ou acceptez le nom par défaut db2apm.

     où *instance_db2_externe* est le nom d'utilisateur de l'instance de serveur Db2 distante que vous avez créée lors de la configuration du serveur Db2 distant.
   - Saisissez le mot de passe pour cet utilisateur *instance_db2_externe*.

   Si vous avez entré 1 et que l'authentification LDAP transparente est configurée pour ce système, l'installation du serveur échoue. Pour plus d'informations, voir «Installation du serveur Cloud APM sur un système informatique où l'authentification LDAP est utilisée», à la page 126.

Si le programme d'installation détecte dans *rép_install*/ccm/depot des packages de configuration d'agent issus d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé les anciens packages et qu'il a créé les nouveaux packages d'agent. Les anciens packages sont nommés *rép_install*/ccm/depot.old.

Si le programme d'installation détecte dans *rép_install* un répertoire keyfiles issu d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé l'ancien répertoire keyfiles et qu'il en a créé un nouveau. L'ancien répertoire keyfiles est nommé *rép_install*/keyfiles.old.L'analyse des prérequis de votre environnement commence et prend un moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Un prérequis comme une bibliothèque manquante ou espace disque insuffisant arrête l'installation. Vous devez corriger le problème et relancer l'installation. Un prérequis «logiciel», tel qu'une mémoire disponible faible, n'entraîne pas l'arrêt de l'installation mais vous devez entrer 1 pour continuer l'installation ou 2 pour l'arrêter. Pour plus d'informations sur les commandes yum provides *nom_fonction* et yum install *nom_fonction*, voir Dépendances. Si l'analyse des prérequis détecte que la base de données RPM est corrompue, la propriété **rpm.dbStatusCorrect** renvoie le statut FAIL. Pour trouver une solution, consultez le forum Cloud Application Performance Management.

Résultats

Le programme d'installation installe les composants du serveur et les fichiers de support ; aucune autre entrée utilisateur n'est requise. Après l'installation du serveur, le programme d'installation configure les composants, ce qui peut prendre jusqu'à 30 minutes ou plus. La partie du processus d'installation qui couvre la création et la configuration des bases de données peut prendre moins de 2 minutes ou plus de 2 heures, selon la vitesse d'entrée-sortie de votre disque dur et la mise en cache d'unité.

Deux agents de serveur, l'agent de surveillance dédié aux événements de transactions et l'agent de surveillance dédié aux événements synthétiques, sont installés et démarrés automatiquement quelle que soit l'offre installée. L'agent Transactions Event fournit des services portant sur le suivi des transactions tandis que l'agent Synthetic Events fournit des services portant sur les transactions synthétiques.

Une fois le serveur Cloud APM installé, vous ne pouvez pas modifier les droits d'accès des fichiers et des répertoires de Cloud APM, ni modifier les propriétaires de groupe ou d'utilisateur de ces fichiers et répertoires.

Que faire ensuite

- Si vous utilisez des noms de base de données personnalisés, veillez à installer le correctif temporaire 5 ou ultérieur du serveur IBM Cloud Application Performance Management, Private V8.1.4.0 après avoir terminé l'installation du serveur Cloud APM. Les correctifs temporaires du serveur Cloud APM V8.1.4 peuvent être téléchargés à partir d'IBM Fix Central.
- Si vous utilisez un serveur Db2 distant avec votre serveur Cloud APM, vérifiez que les exigences suivantes sont satisfaites lors du processus d'installation :
  - Si vous prévoyez d'utiliser Db2 Advanced Enterprise Server Edition V10.5, groupe de correctifs 9 ou Db2 Advanced Workgroup Server Edition V11.1.2, groupe de correctifs 2b ou V11.1.3, groupe de correctifs 3, veillez à installer le correctif temporaire 4 ou ultérieur d'IBM Cloud Application Performance Management Private, V8.1.4.0 après avoir terminé l'installation du serveur Cloud APM. Les correctifs temporaires pour le serveur Cloud APM version 8.1.4 peuvent être téléchargés à partir d'IBM Fix Central
  - Vérifiez que la variable *KQZ_JDBC_JAR_PATHS* est définie sur le chemin d'accès au pilote JDBC du client Db2. Ce chemin d'accès dépend de l'emplacement d'installation d'IBM Data Server Client Db2 que vous avez défini à l'étape 3 de la rubrique «Connexion à un serveur Db2 distant», à la page 129 et de la version de Db2 (10.5 ou 11.1) actuellement utilisée. Si la variable *KQZ_JDBC_JAR_PATHS* n'est pas définie sur le chemin d'accès au pilote JDBC du client Db2, définissez-la maintenant sur ce chemin d'accès et redémarrez l'agent Transaction Event en procédant comme suit :
    - Accédez au répertoire *rép_install*`/serveragents/config`. *rép_install* est le répertoire où le serveur Cloud APM est installé.
    - Sauvegardez le fichier *nomhôte*`_te.cfg`. *nomhôte* correspond au nom d'hôte du serveur Cloud APM.
    - Ouvrez le fichier *nomhôte*`_te.cfg` et recherchez la ligne suivante :

      ```
      KQZ_JDBC_JAR_PATHS=/opt/ibm/db2/version_Db2/java
      ```

      version_Db2 est la version de Db2 installée.
    - Editez le chemin d'accès de sorte qu'il pointe vers l'emplacement des fichiers JAR de votre pilote JDBC. Par exemple, si vous utilisez Db2 V11.1 et qu'IBM Data Server Client est installé dans le répertoire `/opt/ibm` par défaut, le chemin d'accès ressemble à ce qui suit :

      ```
      KQZ_JDBC_JAR_PATHS=/opt/ibm/db2/V11.1/java
      ```
    - Sauvegardez le fichier *nomhôte*`_te.cfg`.
    - Redémarrez l'agent Transaction Event à l'aide de la commande suivante :

      ```
      apm restart txagent
      ```

      L'agent Transaction Event se connecte à la base de données Db2 distante et les seuils sont opérationnels.
  - Le script **install.sh** modifie la taille du pool de mémoire tampon pour `TBSMCFG16KBP` et `TBSMSCR16KBP` et la taille du journal `LOGSECOND`. Ces éléments doivent être redéfinis.

    Pour redéfinir la taille de la mémoire tampon, revenez au DB2 distant et exécutez la commande suivante :

    ```
    db2 connect to SCR32
    db2 UPDATE DATABASE CONFIGURATION FOR SCR32 USING LOGSECOND 25
    db2 alter bufferpool TBSMCFG16KBP IMMEDIATE size 10000
    db2 alter bufferpool TBSMSCR16KBP IMMEDIATE size SCR32_PAGE_COUNT
    db2 disconnect SCR32

    SCR32_PAGE_COUNT
    Nombre de pages de pool de mémoire tampon (pages de 16 K) : 15000 pour Petite, 30000 pour Moyenne
    et 30000 pour Grande.
    ```
- Si vous n'avez pas configuré les images d'installation des agents, du collecteur de données et de la Passerelle hybride (si cette dernière est utilisée) lors de l'installation du serveur, suivez les instructions de la rubrique «Configuration des images téléchargées», à la page 162.

- Si vous souhaitez utiliser les anciens packages de configuration d'agent issus d'une installation précédente pour l'installation d'agent, effectuez les étapes suivantes :
  1. Accédez au répertoire *rép_install*/ccm.
  2. Supprimez le fichier depot.
  3. Changez le nom du fichier depot.old en depot.
- Si vous souhaitez utiliser l'ancien magasin de clés issu d'une installation précédente pour le serveur Cloud APM, effectuez les étapes suivantes :
  1. Accédez au répertoire *rép_install*.
  2. Supprimez le répertoire keyfiles.
  3. Remplacez le nom du fichier keyfiles.old par keyfiles.
  4. Mettez à jour les certificats utilisés par les agents de surveillance pour se connecter au serveur Cloud APM afin qu'ils exploitent le nouveau magasin de clés. Pour plus d'informations, voir «Configuration des certificats entre le serveur et les agents», à la page 222.
  5. Mettez à jour les certificats utilisés par les agents de serveur pour se connecter au serveur Cloud APM afin qu'ils exploitent le nouveau magasin de clés. Pour plus d'informations, voir «Configuration des certificats entre le serveur et les agents», à la page 222.
- Installez les agents sur les systèmes sur lesquels sont installées les applications à surveiller, comme décrit dans la rubrique Chapitre 9, «Installation des agents», à la page 161.
- Configurez le collecteur de données pour déployer la surveillance de vos applications. Pour plus d'informations, voir Chapitre 10, «Configuration de votre environnement», à la page 201.
- Si vous avez oublié le dernier mot de passe correct pour itmuser avant l'installation, exécutez le script qui fournit le mot de passe correct. Voir «Modification d'un mot de passe», à la page 1076.
- Si vous rencontrez des difficultés lors de la réinstallation du serveur après la désinstallation, vérifiez que la désinstallation s'est déroulée correctement. Pour plus d'informations sur la désinstallation du serveur, voir «Désinstallation du serveur», à la page 148.
- Si l'installation du serveur ne progresse pas ou s'achève au bout de 30 minutes (ou plus si la vitesse d'entrée-sortie de votre disque dur est faible), consultez le dernier fichier *rép_install*/ccm/logs/apm-server-*aaaammjj_hhmmss*.log où *rép_install* est le répertoire d'installation du serveur, *aaaammjj* l'année, le mois et le jour, et *hhmmss* l'heure, les minutes et les secondes.
- Si un autre serveur Cloud APM est installé avec des agents qui s'y connectent, vous pouvez modifier les agents sur chaque système géré de sorte qu'ils se connectent au serveur que vous venez d'installer. Pour plus d'informations, voir «Connexion des agents à un autre serveur», à la page 220.
- Si vous avez fait passer le serveur Cloud APM de l'offre Cloud APM, Base à l'offre Cloud APM, Advanced, et si l'Agent WebSphere Applications ainsi quel'Agent Node.js étaient installés et configurés avec l'offre Cloud APM, Base, vous disposez de deux choix pour utiliser les fonctions d'agent avancées que propose l'offre Cloud APM, Advanced :
  – Supprimez l'agent que vous avez installé avec l'offre Cloud APM, Base, puis installez l'agent à nouveau avec l'offre Cloud APM, Advanced. Pour plus d'informations sur la suppression et la réinstallation de l'agent, voir «Désinstallation de vos agents», à la page 187 et Chapitre 9, «Installation des agents», à la page 161.
  – Reconfigurez le collecteur de données. Suivez les instructions ci-dessous pour les différents agents :
    - Agent WebSphere Applications: «Reconfiguration du collecteur de données en cas de modification du type d'offre sur le serveur Cloud APM», à la page 799
    - Agent Node.js: «Configuration du collecteur de données de diagnostic de l'Agent Node.js», à la page 554.
- Le serveur Cloud APM est configuré de sorte à utiliser le registre de base des profils Liberty de WebSphere® Application Server comme méthode par défaut pour l'authentification des utilisateurs. L'utilisateur apmadmin est ajouté au registre de base lors de l'installation et vous pouvez en ajouter d'autres. Pour plus d'informations, voir «Gestion des accès utilisateur», à la page 1020. Cette configuration ne s'applique toutefois qu'aux environnements de test et de démonstration, car le registre de base ne permet ni de verrouiller les comptes utilisateur, ni de contrôler l'expiration des mots de

passe utilisateur. Un serveur LDAP fournit des contrôles de sécurité supplémentaires. Pour les environnements de production, il est recommandé de configurer Cloud APM de sorte à utiliser un serveur LDAP pour l'authentification à la place du registre de base. Pour plus d'informations, voir «Intégration à LDAP», à la page 931.

Désinstallation du serveur

Si vous ne souhaitez plus le serveur Cloud APM sur votre système, vous pouvez le désinstaller.

La procédure ne supprime aucun autre agent de surveillance installé manuellement. Les agents installés automatiquement en tant qu'éléments du serveur Cloud APM sont supprimés. Sont notamment concernés : l'Agent Summarization and Pruning, l'agent Bluemix Integration, l'agent Synthetic Events, et l'agent Transactions Event.

Avant de commencer

Si l'Agent Db2 est installé sur le système du serveur Cloud APM et qu'il surveille la base de données Db2 du serveur Cloud APM, il doit être arrêté avant que vous ne désinstalliez le serveur. Sinon, la désinstallation risque d'échouer. Si vous souhaitez vérifier si l'Agent Db2 est installé sur le système, vous pouvez exécuter la commande de version de l'agent. Pour plus d'informations, voir «Utilisation des commandes de l'agent», à la page 213.

Procédure

Vous devez être le superutilisateur pour désinstaller le serveur.

1. Sur le système sur lequel le serveur Cloud APM est installé, ouvrez l'invite de commande.
2. Exécutez la commande suivante dans le répertoire `/opt/ibm/ccm` (ou `/custom_path/ccm` si vous avez installé le serveur à un autre emplacement) :

   ```
   ./uninstall.sh
   ```
3. Indiquez le répertoire de fichiers journal de désinstallation ou appuyez sur Entrée pour accepter le répertoire par défaut. Le répertoire de fichier journal par défaut est `/tmp/apm/uninstall`.
4. La sortie du programme de désinstallation affiche l'offre Cloud APM que vous pouvez désinstaller, c'est-à-dire soit IBM Cloud Application Performance Management, Base, soit IBM Cloud Application Performance Management, Advanced. Appuyez sur Entrée pour continuer ou saisissez `q` (quitter) pour annuler la désinstallation.

   Remarque : Tous les certificats numériques sont sauvegardés sur *rép_install*`/ccm/`. Il s'agit du seul répertoire qui subsiste après la désinstallation.

Résultats

Les composants du serveur Cloud APM sont désinstallés.

Que faire ensuite

Avant d'essayer de réinstaller votre serveur Cloud APM, vérifiez que la désinstallation a réussi. Le message de sortie `Désinstallation terminée` s'affiche lorsque la désinstallation s'est correctement terminée. Il vous est également possible de vérifier le fichier journal `/tmp/apm/uninstall/apm-server-uninstall_`*aaaammjj_hhmmss*`.log`.

Vous devez également confirmer si la désinstallation de la base de données Db2 a réussi, en recherchant le mot `Success` dans le fichier journal Db2 `/tmp/db2_deinstall.log.`*pid*. Vous trouverez le nom complet de ce fichier journal Db2 (y compris le *pid* à la fin du fichier) dans le fichier journal`/tmp/apm/uninstall/apm-server-uninstall_`*aaaammjj_hhmmss*`.log`. Si la désinstallation de la base de données Db2 a échoué,

nettoyez toutes les entrées Db2. Pour plus d'informations, voir «Nettoyage des entrées Db2».

Nettoyage des entrées Db2

Lors de la désinstallation du serveur Cloud APM, la base de données Db2 peut ne pas se désinstaller correctement. Dans ce cas, nettoyez les entrées Db2 avant de tenter de réinstaller le serveur Cloud APM.

Avant de commencer

Si vous êtes connecté à une base de données Db2 distante, aucune action supplémentaire n'est nécessaire. Si vous avez installé une base de données Db2 pendant l'installation du serveur Cloud APM, consultez le fichier journal `/tmp/db2_deinstall.log.pid` pour déterminer si la désinstallation de la base de données Db2 a échoué. Si tel est le cas, exécutez la procédure suivante :

Procédure

1. Exécutez la commande suivante ::
   ```
   ps aux | grep db2
   ```
2. Arrêtez tous les processus Db2 en cours d'exécution qui sont renvoyés par la commande **ps**, en entrant la commande suivante :
   ```
   kill -9 <processID>
   ```
3. Supprimez tous les utilisateurs Db2 (par exemple, les utilisateurs dasusr1, db2apm, db2fenc1, itmuser) via la commande suivante :
   ```
   userdel -r <username>
   ```
4. Accédez au répertoire `/var` et supprimez le répertoire `/var/db2`.
5. Editez le fichier `/etc/services`, puis supprimez tous les services Db2 (les derniers services dans le fichier, précédés du préfixe db2).

Résultats

Les entrées Db2 sont nettoyées et vous pouvez réinstaller votre serveur Cloud APM. Pour plus d'informations, voir Chapitre 7, «Installation du serveur», à la page 125.

Scanner de prérequis

Une fois que vous avez lancé le script d'installation du serveur Cloud APM, un scanner préliminaire se lance automatiquement et affiche ses résultats. Le scanner affiche un chemin d'accès à un fichier journal que vous pouvez consulter si l'un des prérequis n'est pas satisfait. Vous devez corriger tous les prérequis non satisfaits avant de relancer l'installation.

Un prérequis «logiciel», tel qu'une mémoire disponible faible, n'entraîne pas l'arrêt de l'installation mais est signalé dans les résultats. Une bibliothèque obsolète ou un espace disque insuffisant entraîne l'arrêt du processus d'installation. La configuration minimale requise pour l'installation est indiquée dans le tableau 11, à la page 93 et le tableau 12, à la page 94 dans «Configuration matérielle requise pour le serveur Cloud APM», à la page 92. Reportez-vous à la colonne «Petite» dans le tableau pour connaître l'offre applicable.

L'exemple suivant de résultats du scanner de prérequis indique où les contrôles des prérequis ont échoué. Vous devez rectifier les problèmes détectés et redémarrer l'installation. (Voir «Conseils pour la résolution des dépendances non satisfaites», à la page 83.)

```
Version : 1.2.0.18
    Build  : 20160602
    OS name: Linux
  User name: root
```

```
 Machine Information
 Machine name: somehost
 Serial number:  ...


Scenario: Prerequisite Scan

KIM - IBM Monitoring [version 01020006]:
Property                                Result   Found                                    Expected
========                       ======    =====                          ========
Memory                         WARN      3.48GB                         12-16GB
Disk                                 FAIL      14.00GB                          100GB
os.swapSize                          WARN      3.81GB                           2-4GB
numLogicalCPU                        WARN      2                                4
db2.usersNotPresent            FAIL      db2fenc1,dasusr1               dasusr1, db2apm, db2fenc1, itmuser
db2.groupsNotPresent           FAIL      db2iadm1,db2fadm1              db2iadm1,db2fadm1,dasadm1
os.isUnixServiceRunning.crond FAIL         False            True
os.lib.pam_32                        FAIL      Unavailable                      regex{libpam.so.*}
os.package.sg3_utils                 FAIL      Unavailable                      sg3_utils

Aggregated Properties for Scanned Products:
Property                                Result   Found                                    Expected
========                       ======    =====                          ========
/                                    FAIL      14.00GB                           100.00GB
Memory                         WARN      3.48GB                         12.00-16.00GB

Overall result:   FAIL
Detailed results are also available in /tmp/smai_prs_20141203_053249/result.txt
```

Voir la section tableau 5, à la page 72 du chapitre «Eléments prérequis pour serveur Cloud APM», à la page 72 pour obtenir une liste des prérequis vérifiés, comprendre les conséquences d'un échec pour chaque prérequis, et connaître les actions à entreprendre pour corriger chaque échec.

Exécution manuelle du scanner de prérequis

Lorsque vous installez le serveur Cloud APM, une analyse des prérequis de votre environnement, qui nécessite un certain temps, est lancée. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec.

Vous pouvez entrer une commande de contrôle des prérequis à tout moment avant d'installer le serveur Cloud APM.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la configuration requise pour le serveur Cloud APM, voir Chapitre 4, «Configuration requise», à la page 71.

Procédure

1. Pour télécharger et extraire les fichiers d'installation du serveur depuis IBM Passport Advantage, suivez les étapes 1, à la page 142 à 5, à la page 142 décrites dans la rubrique *Téléchargement et installation du serveur*.
2. Accédez au répertoire dans lequel vous avez extrait les fichiers d'installation du serveur.
3. Exécutez le scanner de prérequis :
   - Pour exécuter le scanner de prérequis avec invites, suivez ces étapes :
     a. Entrez la commande suivante :

        ```
        ./install.sh -p code_produit
        ```

        où

code_produit
Indique si le serveur Db2 est installé localement ou à distance. Une valeur de `IPDB2` spécifie une analyse des prérequis pour une installation du serveur Cloud APM avec un serveur Db2 local (option par défaut). Une valeur de `IPM` spécifie une analyse des prérequis pour une installation du serveur Cloud APM avec un serveur Db2 externe (voir «Connexion à un serveur Db2 distant», à la page 129).

b. A l'invite de commande, entrez le répertoire d'installation ou acceptez la valeur par défaut.

- Pour exécuter le scanner de prérequis sans invites, entrez :

  ```
  ./install.sh -p code_produit -d rép_install
  ```

  Par exemple :

  ```
  ./install.sh -p IPM -d /root/nondefault/dir
  ```

Résultats

Le scanner de prérequis imprime les résultats. Les résultats possibles de l'exécution du scanner de prérequis sont les suivants :

PASS Si l'environnement cible satisfait tous les contrôles des prérequis, l'analyse renvoie un résultat `PASS` global pour l'environnement.

WARN
Si l'environnement cible ne satisfait pas des exigences considérées comme «mineures» et qu'aucun prérequis n'affiche le statut FAIL, l'installation peut se poursuivre. Toutefois, les performances du serveur risquent de ne pas être optimales.

FAIL Si l'environnement cible ne satisfait aucun des contrôles des prérequis, l'analyse renvoie un résultat `FAIL` global pour l'environnement. Prenez les mesures appropriées. Par exemple, installez les packages de système d'exploitation manquants ou augmentez l'espace disque.

Que faire ensuite

Exécutez le script d'installation pour installer le serveur Cloud APM.

Contournement de l'analyse des prérequis

Lorsque vous installez le serveur Cloud APM, l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Vous pouvez entrer une commande pour ignorer le contrôle prérequis.

Il est recommandé d'activer l'analyse des prérequis mais, pour certains scénario de test, vous pouvez l'ignorer pour gagner du temps.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez téléchargé et extrait les fichiers d'installation, effectuez cette étape pour ignorer l'analyse des prérequis.

Procédure

Sur le système où vous prévoyez d'installer le serveur, entrez la commande suivante :

```
export SKIP_PRECHECK=YES
```

Que faire ensuite

Exécutez le script d'installation pour commencer à installer le serveur sans l'analyse des prérequis.

Installation d'une base de données MongoDB distante

MongoDB est une base de données open source NoSQL installée avec le serveur Cloud APM. MongoDB stocke les données de la fonction de suivi de transaction fournie avec l'offre, ainsi que les données d'événement de seuil. Vous pouvez installer et configurer MongoDB sur un système distant à partir du serveur.

Dans les environnements étendus, une base de données MongoDB externe peut être utilisée pour réduire la charge au niveau du serveur.

Avant de commencer

Pour vérifier la disponibilité du MongoDB installé avec le serveur Cloud APM, saisissez `/usr/bin/apm status mongodb`. Le résultat `Service mongodb started (PID 7574)` indique que MongoDB est installée avec le serveur Cloud APM. Le répertoire d'installation de MongoDB est *rép_install*`/mongodb` (`/opt/ibm/mongodb` par défaut). MongoDB nécessite un port TCP qui doit être disponible ; il est vérifié au cours du contrôle des prérequis : 27000.

Vérifiez que le service cron est en cours d'exécution sur le système externe. La base de données MongoDB utilise ce service pour ses travaux cron.

Pourquoi et quand exécuter cette tâche

Utilisez cette procédure pour effectuer les tâches suivantes :

- Installez la base de données MongoDB sur un système distinct du serveur Cloud APM.
- Configurez les communications entre la base de données MongoDB et le serveur.
- Désactivez la base de données MongoDB installée en local avec le serveur.

Pour connaître la version prise en charge de MongoDB, voir la rapport de la configuration système requise pour votre offre sur System requirements (APM Developer Center). La version prise en charge est disponible depuis l'onglet Prerequisites du rapport.

Procédure

1. Copiez le contenu du répertoire `packages/MongoDB` depuis l'image d'installation du serveur vers le système distant.
2. Installez et activez MongoDB sur un système distant :
   a. Sur le système distant, basculez vers le répertoire où vous avez téléchargé le répertoire MongoDB et exécutez l'une des commandes suivantes :
      - Pour installer MongoDB dans le répertoire `/opt/ibm/mongodb` par défaut :
        ```
        install-mongodb.sh
        ```
      - Pour installer MongoDB dans un autre répertoire :
        ```
        install-mongodb.sh /custom/path
        ```
        où */custom/path* est le chemin d'accès et le répertoire spécifiés.
   b. Exécutez la commande suivante :
      ```
      activate-mongodb.sh
      ```
   MongoDB est configurée et démarrée.
3. Configurez les communications entre la base de données MongoDB distante et le serveur Cloud APM :
   a. Le cas échéant, connectez-vous à la console Cloud APM. (Voir «Démarrage de la console Cloud APM», à la page 989.)

b. Cliquez sur **Configuration système** > **Configuration avancée**, puis sur **Mongo Configuration** (Configuration Mongo).
c. Dans la zone **Nom d'hôte**, entrez l'adresse IP ou le nom d'hôte complet du système distant où MongoDB est installée.
d. Cliquez sur **Sauvegarder** pour sauvegarder la configuration.

Après avoir cliqué sur **Sauvegarder**, les composants de suivi de transaction commencent à communiquer avec la base de données MongoDB distante.

4. Arrêtez la base de données MongoDB qui a été installée avec le serveur Cloud APM, puis désactivez les travaux cron et le redémarrage automatique de la base de données MongoDB après le redémarrage, en exécutant la commande suivante sur le système où le serveur Cloud APM est installé :

```
rép_install/mongodb/bin/deactivate-mongodb.sh
```

où *rép_install* est le répertoire d'installation `/opt/ibm/` par défaut du serveur ou le répertoire personnalisé que vous avez spécifié lors de l'installation du serveur.

5. Pour activer la base de données MongoDB distante pour le transfert des données d'événement de seuil et de suivi de transaction vers serveur Cloud APM, exécutez la commande suivante sur le système du serveur Cloud APM :

```
touch rép_install/mongodb/mongodb-remote
```

Résultats

La base de données MongoDB installée avec le serveur Cloud APM est désactivée, tandis que les données d'événement de seuil et de suivi de transaction sont transférées entre le serveur et la base de données MongoDB distante.

Tous les *nouveaux* événements de seuil et les *nouvelles* données de suivi de transaction sont transférés entre serveur Cloud APM et la base de données MongoDB distante.

Les événements ouverts et les données de suivi de transaction qui existent ne sont pas migrés vers la nouvelle base de données MongoDB. Pour afficher les événements ouverts existants dans la console Cloud APM, utilisez la commande **touch** de Linux afin de modifier la date et l'heure de tous les fichiers `private_situation.xml` des sous-répertoires sous le répertoire *rép_install*`/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source`.

Que faire ensuite

MongoDB est initialement configurée avec deux ID utilisateur qui se partagent le même mot de passe mongoUsrpasswd@08 par défaut : **admin**, qui est associé au rôle MongoDB *userAdmin* autorisé à gérer les comptes utilisateur MongoDB et **user**, qui ne possède aucun droit particulier. Vous pouvez exécuter le script `mongopasswd.sh` pour modifier simultanément le mot de passe des deux utilisateurs.

Concepts associés:

«Mots de passe et ID utilisateur des composants», à la page 1075
Divers composants requièrent des ID utilisateur et des mots de passe pour y accéder.

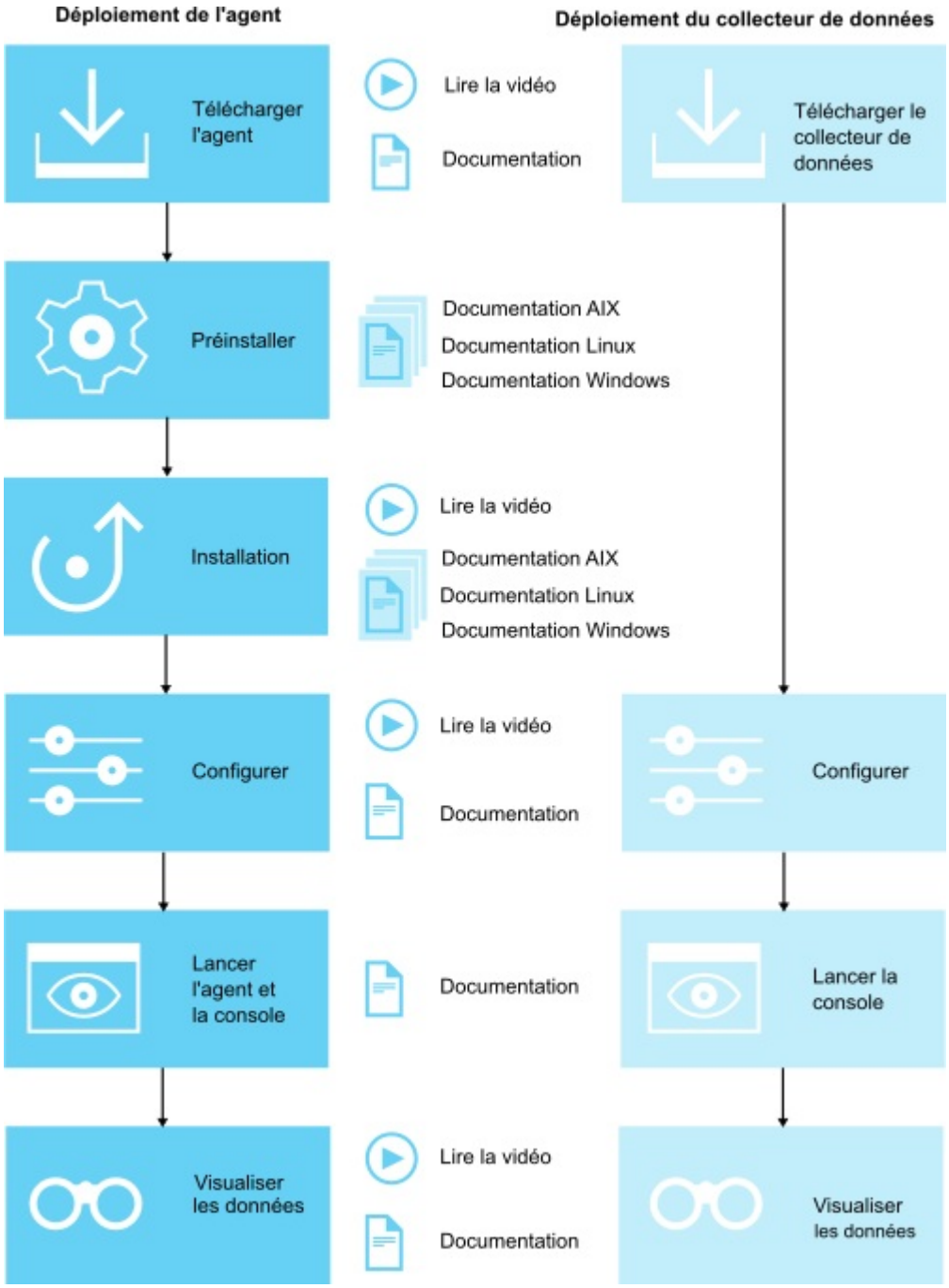
Tâches associées:

«Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090
Utilisez les commandes de vérification du statut, de démarrage, d'arrêt et de recyclage des composants du serveur Cloud APM lorsque cela est nécessaire pour les tâches de maintenance et d'identification et de résolution des problèmes.

«Basculement vers une base de données MongoDB locale», à la page 1099
Si votre serveur Cloud APM est connecté à une base de données MongoDB sur un serveur distant, vous pouvez à tout moment basculer sur la base de données MongoDB locale.

Chapitre 8. Déploiement d'agents et de collecteurs de données

Selon les agents, les tâches nécessaires entre l'installation et l'affichage des données qu'ils collectent varient. Certaines tâches sont automatiques, d'autres sont manuelles. Après avoir téléchargé vos collecteurs de données, vous devez configurer manuellement chaque collecteur de données.



© Copyright IBM Corp. 2015, 2018

Après l'installation, certains agents sont configurés et démarrés automatiquement
Tout agent démarré est configuré avec les paramètres par défaut. Pour déterminer quels agents sont configurés et démarrés manuellement, voir tableau 23.

Après l'installation, certains agents nécessitent une configuration manuelle mais démarrent automatiquement
Pour plus d'informations sur la configuration de vos agents, voir Chapitre 10, «Configuration de votre environnement», à la page 201. Pour déterminer quels agents sont configurés manuellement et démarrés automatiquement, voir tableau 23.

Après l'installation, certains agents doivent être configurés et démarrés manuellement
Tout agent qui n'est pas démarré automatiquement doit être configuré pour pouvoir être démarré. Pour déterminer quels agents sont configurés et démarrés manuellement, voir tableau 23.

Les agents multi-instances nécessitent la création d'une première instance et un démarrage manuel
Vous devez créer la première instance et démarrer l'agent manuellement. Un agent multi-instance implique qu'une installation unique de l'agent instancie une instance de surveillance unique pour chaque instance d'application. Vous pouvez afficher ces instances depuis la console Cloud APM. Pour déterminer quels agents sont des agents multi-instances, voir tableau 23.

Agents de système d'exploitation et surveillance des fichiers journaux
L'Agent Linux OS, l'Agent UNIX OS et l'agent Windows OS sont configurés et démarrés automatiquement. Toutefois, vous pouvez configurer la surveillance des fichiers journaux pour les agents de système d'exploitation afin de pouvoir surveiller les fichiers journaux d'application. Pour plus d'informations, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 590.

Déploiement d'agents d'agent et de collecteur de données

Tableau 23. Liste de contrôle post-installation

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent Amazon EC2	—	—	—	✓
agent Amazon ELB	—	—	—	✓
Agent Azure Compute	—	—	—	✓
agent Cassandra	—	—	✓	✓
agent Cisco UCS	—	—	✓	✓
agent Citrix VDI	—	—	—	✓
agent DataPower	—	—	—	✓
Agent DataStage	—	—	✓	✓
Agent Db2	—	—	—	✓
agent Hadoop	—	—	✓	—
agent HMC Base	—	—	—	✓

Tableau 23. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent HTTP Server	✓ Vous devez vérifier le fichier de configuration créé par l'agent pour le serveur HTTP. Vous devez ensuite ajouter manuellement la configuration du collecteur de données au fichier de configuration du serveur.	—	—	—
agent IBM Integration Bus	—	—	—	✓
Internet Service Monitoring	✓	—	—	—
collecteur de données J2SE	—	✓	—	—
agent JBoss	—	—	—	✓
collecteur de données Liberty	—	✓	—	—
Agent Linux KVM	—	—	✓	✓
Agent Linux OS	✓	—	—	—
agent Microsoft Active Directory	—	✓ Cet agent est démarré automatiquement. Vous devez cependant le configurer pour afficher les données de certains attributs.	—	—
agent Microsoft Cluster Server	—	—	✓	—
agent Microsoft Exchange Server	—	✓ Cet agent est démarré automatiquement. Vous devez cependant le configurer pour afficher les données de tous les attributs.	—	—

Tableau 23. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent Microsoft Hyper-V Server	✓	—	—	—
agent Microsoft IIS	✓	—	—	—
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	✓	✓ Cet agent est démarré automatiquement. Vous devez cependant le configurer pour afficher les données de certains attributs.	—	—
agent Microsoft Office 365	—	—	✓	—
agent Microsoft .NET	—	✓ Le collecteur de données doit être configuré avant le signalement des données.	—	—
agent Microsoft SharePoint Server	✓	—	—	—
agent Microsoft SQL Server	—	—	—	✓ Chaque instance d'agent doit être configurée et démarrée manuellement.
Agent MQ Appliance	—	—	—	✓
Agent MongoDB	—	—	—	✓
Agent MySQL	—	—	—	✓
agent NetApp Storage	—	—	✓	✓
Agent Node.js	—	✓ L'agent doit être configuré avant le signalement des données. Vous devez ajouter un plug-in de surveillance à votre application Node.js.	—	—
collecteur de données Node.js	—	✓	—	—

Tableau 23. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
Agent OpenStack	—	—	✓	✓
Agent Oracle Database	—	—	—	✓
Agent PHP	—	—	—	✓
Agent PostgreSQL	—	—	—	✓
collecteur de données Python	—	✓	—	—
agent RabbitMQ	—	—	✓	✓
Agent de surveillance des temps de réponse	✓	—	—	—
Agent Ruby	—	—	—	✓ Pour des diagnostics approfondis, l'agent doit être configuré avant le signalement des données. Pour activer les tableaux de bord de diagnostic, vous devez installer et configurer le collecteur des données de diagnostic.
collecteur de données Ruby	—	✓	—	—
Agent SAP	—	—	✓	✓
Agent SAP HANA Database	—	—	✓	✓
Agent SAP NetWeaver Java Stack	—	—	✓	✓
agent Siebel	—	—	—	✓
Agent Sterling Connect Direct	—	—	—	✓
Agent Sterling File Gateway	—	—	✓	✓
agent Sybase	—	—	✓	✓

Tableau 23. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
Agent Synthetic Playback		✓ L'agent est démarré automatiquement mais l'agent doit être configuré pour des applications privées internes. Les transactions doivent être créées dans Synthetic Script Manager avant la transmission des données.	—	✓
Agent Tomcat	—	—	—	✓
Agent UNIX OS	✓	—	—	—
Agent VMware VI	—	—	✓	✓
Agent WebLogic	—	—	—	✓
Agent WebSphere Applications	—	✓ L'agent est démarré automatiquement mais le collecteur de données doit être configuré avant le signalement des données.	—	—
Agent WebSphere Infrastructure Manager	—	—	—	✓
Agent WebSphere MQ	—	—	—	✓
agent Windows OS	✓	—	—	—

Chapitre 9. Installation des agents

Installez les agents de surveillance sur les systèmes où se trouvent les applications correspondantes que vous souhaitez surveiller. Pour les agents prenant en charge la surveillance éloignée, vous pouvez installer ces agents sur un ordinateur différent de celui sur lequel se trouve la ressource. Les collecteurs de données autonomes ne requièrent pas d'installation.

Si vous choisissez des collecteurs de données autonomes pour surveiller vos applications, vous pouvez ignorer la procédure d'installation. Toutefois, vous devez au préalable configurer les images de collecteur de données téléchargées pour les communications entre le serveur Cloud APM et les collecteurs de données. Si vous n'avez pas sélectionné l'option de configuration des images de collecteur de données lors de l'installation du serveur, suivez les instructions de la rubrique «Configuration des images téléchargées», à la page 162 pour configurer l'image téléchargée. Sinon, passez à la rubrique Chapitre 10, «Configuration de votre environnement», à la page 201 pour des instructions sur la manière de configurer les collecteurs de données pour la surveillance de vos applications.

Surveillance éloignée

Certains agents peuvent être installés à distance à partir de la ressource qu'ils surveillent. Les agents suivants prennent en charge la surveillance éloignée :

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower : cet agent ne peut être installé que sur un ordinateur distant.
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss : si vous souhaitez utiliser cet agent pour la surveillance des ressources, installez-le à distance ou en local. Si vous souhaitez utiliser l'agent pour le suivi des transactions et les diagnostics Deep Dive, installez-le en local.
- Monitoring Agent for Linux KVM
- Monitoring Agent for Microsoft Cluster Server
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Microsoft SharePoint Server
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications

© Copyright IBM Corp. 2015, 2018

- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack : si vous souhaitez utiliser cet agent pour la surveillance des ressources, installez-le à distance ou en local. Si vous souhaitez utiliser l'agent pour le suivi des transactions et les diagnostics Deep Dive, installez-le en local.
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic : si vous souhaitez utiliser cet agent pour la surveillance des ressources, installez-le à distance ou en local. Si vous souhaitez utiliser l'agent pour le suivi des transactions et les diagnostics Deep Dive, installez-le en local.
- Agent de surveillance des temps de réponse : si vous utilisez le composant Analyseur de paquet, installez l'agent à distance ou en local. Si vous utilisez le module Temps de réponse IBM HTTP Server, installez l'agent sur le même ordinateur que celui de HTTP Server.

Configuration des images téléchargées

Pour installer des agents ou la Passerelle hybride d'IBM Cloud Application Performance Management ou encore configurer le collecteur de données, vous devez configurer les images téléchargées afin d'établir la communication avec le serveur Cloud APM.

Si vous avez déjà configuré vos images téléchargées, mais souhaitez basculer du protocole HTTP au protocole HTTPS, vous pouvez configurer les images de sorte à spécifier HTTP ou HTTPS.

Avant de commencer

Avant de configurer l'image d'installation de l'agent pour Linux for Power Systems (Big Endian), veillez à appliquer le correctif temporaire 8.1.4.0 Core Framework APM IF06 sur le serveur Cloud APM. Ce module de correction peut être téléchargé depuis IBM Fix Central.

Pourquoi et quand exécuter cette tâche

Si vous avez sélectionné l'option de configuration de vos images téléchargées lorsque vous avez installé le serveur, vous pouvez ignorer cette tâche.

Avant de pouvoir installer les agents, vous devez configurer les images d'installation de l'agent téléchargées pour initier la communication avec le serveur Cloud APM. L'infrastructure d'agent n'est pas incluse dans les images d'installation de l'agent téléchargées. L'infrastructure d'agent est installée dans le répertoire `AgentFrameworks` au cours de l'installation du serveur Cloud APM. L'infrastructure d'agent est injectée dans les images d'installation pendant la configuration.

La configuration des images téléchargées pour établir une connexion avec le serveur Cloud APM requiert l'exécution de deux scripts :

- Exécutez **`make_configuration_packages`** sur le système où le serveur Cloud APM est installé. Le script crée un fichier TAR correspondant au module de configuration et un fichier compressé contenant les informations dont le programme d'installation et les agents ou les collecteurs de données ont besoin pour établir des communications avec le serveur.
- Exécutez **`configure_agent_images`** sur le système où le serveur Cloud APM est installé. Le script applique les informations du module de configuration aux fichiers image téléchargés pour l'installation des agents ou le déploiement du collecteur de données.

Vous pouvez décider de ne pas décompresser les images avant d'exécuter les scripts ou choisir de les décompresser à l'avance. Vous pouvez également décider d'exécuter les scripts en mode interactif en répondant aux invites du système pour exécuter chaque procédure, ou lancer l'exécution en mode de traitement par lots en ajoutant des arguments de ligne de commande.

Procédure

Pour télécharger et configurer les images téléchargées, procédez comme suit :

1. Téléchargez les images d'agent, du collecteur de données ou de la Passerelle hybride sur un serveur Cloud APM (voir Chapitre 6, «Instructions de téléchargement», à la page 115).
2. Créez les fichiers du module de configuration en exécutant le script de création du module de configuration en mode interactif ou de traitement par lots :
   - Exécutez le script de création du module de configuration en mode interactif :
     a. Sur le système sur lequel le serveur Cloud APM est installé, accédez au répertoire `/opt/ibm/ccm` par défaut ou au répertoire *chemin_personnalisé*`/ccm` spécifié au cours de l'installation du serveur, puis entrez la commande suivante :

        ```
        ./make_configuration_packages.sh
        ```

     b. Lorsque vous y êtes invité, entrez l'adresse IP ou le nom d'hôte du serveur Cloud APM auquel l'agent, le collecteur de données ou la passerelle hybride doit se connecter, ou acceptez la valeur par défaut.
     c. Entrez le répertoire dans lequel le module de configuration doit être stocké une fois créé ou acceptez la valeur par défaut `/opt/ibm/ccm/mkcustpkg_workdir.`*ID_processus_script*.
     d. Sélectionnez le protocole de communication. Pour des communications sécurisées, sélectionnez le protocole HTTPS. Pour des communications non sécurisées, sélectionnez le protocole HTTP. Le protocole de communication entre le serveur et les agents ou les collecteurs de données doit être le même. Pour plus d'informations, voir «Définition des communications HTTP ou HTTPS», à la page 128.
   - Exécutez le script en mode de traitement par lots en entrant la commande suivante :

     ```
      ./make_configuration_packages.sh -s ip_serveur
     [-p protocole_communication] [-k rép_fichier_de_clés] [-d rép_module_config]
      [-n]
     ```

     -s ***ip_serveur***
     (Obligatoire) Adresse IP ou nom de domaine complet du serveur.

     -p ***protocole_communication***
     (Facultatif) Les valeurs possibles sont `http` et `https`. Le protocole de communication utilisé par défaut est HTTP. Si vous avez défini le protocole sécurisé HTTPS avant d'installer le serveur, entrez **`-p https`** pour remplacer le protocole des agents ou des collecteurs de données par HTTPS afin qu'il corresponde à ce qui a été défini pour le serveur. Pour plus d'informations, voir «Définition des communications HTTP ou HTTPS», à la page 128.

     -k ***rép_fichier_de_clés***
     (Facultatif) Chemin d'accès aux fichiers de clés devant être utilisés avec les agents. L'option -k est nécessaire uniquement si vous avez créé un certificat personnalisé pour la connexion HTTPS entre l'agent et le serveur («Configuration d'un certificat autosigné», à la page 223 ou «Configuration d'un certificat personnalisé d'une autorité de certification racine tierce pour les communications d'agent HTTPS», à la page 227).

     -d ***rép_module_config***
     (Facultatif) Chemin d'accès au répertoire dans lequel vous souhaitez stocker le module de configuration une fois celui-ci créé.

     -n (Facultatif) Ne validez pas les paramètres d'entrée utilisés dans la configuration de l'agent, par exemple, le nom d'hôte du serveur.

   Le fichier du module de configuration `onprem_config.tar` est créé dans le répertoire par défaut ou le répertoire que vous avez indiqué.
3. Configurez les images téléchargées (agent, collecteur de données ou Passerelle hybride) sur un système Linux en mode interactif ou en mode de traitement par lots. Vous pouvez configurer l'image

avant ou après l'extraction des fichiers image. Pour les systèmes AIX, exécutez le script sur un système Linux, de préférence sur le serveur Cloud APM, puis copiez le fichier archive des images configuré dans votre système AIX.

- Exécutez le script de configuration des images en mode interactif :
  a. Exécutez la commande suivante :
     ```
     ./configure_agent_images.sh
     ```
  b. Si vous avez décompressé les images téléchargées, entrez le chemin d'accès au répertoire dans lequel vous avez décompressé l'image.
  c. Si vous n'avez pas décompressé les images téléchargées, entrez le chemin d'accès au répertoire dans lequel vous avez téléchargé le fichier archive.
  d. Si vous n'avez pas décompressé les images téléchargées, entrez le chemin d'accès au répertoire dans lequel vous souhaitez stocker le fichier archive des images configurées. Utilisez le chemin d'accès par défaut suivant ou spécifiez un autre chemin d'accès :
     ```
     /opt/ibm/ccm/depot
     ```
  e. Si vous exécutez le script dans un environnement où l'infrastructure d'agent n'est pas disponible à l'emplacement par défaut, *rép_install_serveur*/ccm/AgentFrameworks, entrez le chemin d'accès au répertoire contenant les infrastructures d'offre d'agent décompressées.
- Exécutez le script de configuration des images en mode de traitement par lots en entrant la commande suivante :
  ```
  ./configure_agent_images.sh -p rép_module_config
  -s rép_images_téléchargées [-a rép_infrastructures_agent] [-d rép_images_configurées]
  ```

  -p ***rép_module_config***
  Obligatoire. Si vous n'avez pas décompressé le module de configuration, entrez le chemin d'accès au répertoire dans lequel se trouve le module de configuration.

  -s ***rép_images_téléchargées***
  Obligatoire. Chemin d'accès au répertoire dans lequel vous avez téléchargé le fichier archive des images. Si vous avez décompressé les images, cette variable représente le chemin d'accès au répertoire qui contient les images d'agent ou du collecteur de données décompressées.

  -a ***rép_infrastructures_agent***
  Facultatif. Répertoire contenant les modules des infrastructures d'offre d'agent décompressés. Ces fichiers sont disponibles par défaut dans le répertoire *rép_install_serveur*/ccm/AgentFrameworks sur le serveur Cloud APM. Si des modules d'infrastructures d'offre d'agent par défaut sont utilisés, cette variable n'est pas obligatoire.

  -d ***rép_images_configurées***
  Facultatif. Si vous n'avez pas décompressé le fichier archive des images, cette variable représente le chemin d'accès au répertoire dans lequel vous souhaitez stocker le fichier archive des images d'agent ou du collecteur de données configurées.

  -h Affiche l'aide pour la commande **configure_agent_images.sh**.

Si un message indique qu'une ou plusieurs images d'agent sont ignorées, mettez à niveau votre installation serveur. Ensuite, exécutez le script de configuration des images d'agent. Pour plus d'informations, voir «Mise à niveau de votre serveur», à la page 941.

Résultats

Le programme d'installation configure les images ou le fichier archive des images pour l'agent ou le collecteur de données. Un message d'état indique que les images ou le fichier archive des images sont configurés et précise l'emplacement des fichiers.

Que faire ensuite

- Pour les images d'agent, reportez-vous aux rubriques «Installation des agents sur les systèmes AIX», «Installation des agents sur les systèmes Linux», à la page 170 ou «Installation des agents sur les systèmes Windows», à la page 177.

  Si vous avez configuré le fichier archive des images d'agent sur le serveur Cloud APM, copiez le fichier archive des images d'agent configurées sur le système sur lequel les applications à surveiller sont installées, puis installez les agents.
- Pour l'image de la Passerelle hybride, reportez-vous à la rubrique «Installation de la passerelle hybride», à la page 878.

  Si vous avez configuré le fichier archive de l'image de la Passerelle hybride sur le serveur Cloud APM, copiez le fichier archive de l'image configurée sur le système de votre réseau Tivoli Monitoring sur lequel vous souhaitez installer la Passerelle hybride.
- Pour les images du collecteur de données, reportez-vous à l'une des rubriques suivantes selon le type des applications que vous souhaitez surveiller :
  - «Configuration de la surveillance de J2SE», à la page 418
  - «Configuration de la surveillance de Node.js», à la page 548
  - «Configuration de la surveillance Python», à la page 623
  - «Configuration de la surveillance de Ruby», à la page 669
  - «Configuration de la surveillance des applications WebSphere», à la page 765

Installation des agents sur les systèmes AIX

Installez les agents de surveillance sur vos systèmes AIX pour les ressources que vous souhaitez gérer.

- Monitoring Agent for DataPower
- Monitoring Agent for Cassandra
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for MQ Appliance
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Agent de surveillance des temps de réponse

Préinstallation sur les systèmes AIX

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes AIX. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter aux exigences identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Installation en tant qu'utilisateur non superutilisateur
Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation. Autrement, l'installation est annulée. Pour plus d'informations sur l'installation en tant qu'utilisateur non superutilisateur, voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 183.

Limitation à 70 caractères pour le chemin d'installation
Le répertoire d'installation et son chemin d'accès ne doivent pas comporter plus de 70 caractères.

AIX uniquement : limitation à 100 caractères pour les noms de fichier `.tar`
La commande par défaut **`tar`** sur des systèmes AIX ne peut pas traiter les noms de fichiers comportant plus de 100 caractères. Pour éviter les problèmes d'installation, procédez comme suit :

1. Téléchargez et installez la version GNU de la commande **`tar`** à partir du site Web AIX Toolbox for Linux Applications.
2. Faites de la version GNU votre commande **`tar`** par défaut. Effectuez l'une des étapes suivantes :
   - Dans la variable d'environnement *PATH*, insérez d'abord la variable suivante :
     ```
     export PATH=/opt/freeware/bin:$PATH
     ```
   - Remplacez `/bin/tar` par le lien symbolique vers `/opt/freeware/bin/tar`

Sinon, effectuez une mise à niveau vers la dernière version d'AIX pour recevoir le correctif du code pour les noms de fichier comportant plus de 100 caractères. Pour plus de détails, voir la note technique relative à la commande TAR pour AIX V6.1 ou la note technique relative à la commande TAR pour AIX V7.1.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

agent DataPower
Avant l'installation de l'agent, le programme de vérification des prérequis vérifie que le paramètre *ulimit* correspond à **`unlimited`** sous AIX. Vous devez exécuter la commande **`ulimit -d unlimited`** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **`unlimited`**. Cet agent ne peut pas être installé sur la même machine que le dispositif DataPower à surveiller.

agent HMC Base
Si vous prévoyez d'installer l'agent en tant que superutilisateur, vous devez vous assurer que le système TL07 est installé. Si vous prévoyez d'installer l'agent en tant qu'utilisateur non superutilisateur, vous devez vous assurer que le système TL08 est installé pour AIX version 6 uniquement.

agent HTTP Server
Installez et exécutez cet agent en tant que superutilisateur. Utilisez le même ID utilisateur pour installer et exécuter l'agent. Si vous installez et exécutez l'agent en tant qu'utilisateur non superutilisateur, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître IBM HTTP Server.

L'installation échoue sous AIX car la commande **.tar** par défaut tronque les chemins longs sur le système AIX. Pour plus d'informations, consultez la section «Limitation à 100 caractères pour les noms de fichier `.tar`» dans la présente rubrique.

AIX uniquement : installez l'utilitaire lynx ou l'application curl.

Agent Oracle Database

Sous Red Hat Enterprise Linux version 5 et version 6 et SUSE Linux Enterprise Server version 11 et version 12 x64, si l'Agent Oracle Database surveille la base de données Oracle à distance, vous devez commencer par installer les clients Oracle Instant. Installez les clients Oracle Instant à partir de la page Téléchargements Oracle Technology Network - Instant Client.

Les clients Instant v10.x ,v11.x et v12.x sont pris en charge par l'Agent Oracle Database.

Agent de surveillance des temps de réponse

Avant d'installer l'Agent de surveillance des temps de réponse, passez en revue la section relative à la planification de l'installation ici : «Planification de l'installation», à la page 640.

Agent SAP HANA Database

1. Installez le client de base de données SAP HANA HDBSQL version 1.00.102.06 ou ultérieure sur le système AIX.
2. Exécutez la commande suivante pour ajouter le chemin du répertoire d'installation à la variable d'environnement **LIBPATH**.

   `export LIBPATH=$LIBPATH:`*`chemin_répertoire_install`*

   Exemple : `export LIBPATH=$LIBPATH:/usr/sap/hdbclient`, où `/usr/sap/hdbclient` indique le chemin d'installation du client de base de données SAP HANA.

Important :

Si le chemin d'installation du client de base de données SAP HANA n'est pas ajouté à la variable d'environnement **LIBPATH** le scanner de prérequis renvoie le résultat `FAIL`.

La variable d'environnement que vous avez ajoutée à l'aide de la commande export est conservée uniquement pour une session donnée du terminal. Par conséquent, assurez-vous d'avoir exécuté le script d'installation de l'agent depuis le même terminal que celui utilisé pour ajouter la variable d'environnement.

Agent WebSphere Applications

Avant l'installation de l'agent, le programme de vérification des prérequis vérifie que le paramètre *ulimit* est défini sur **524000** sur le système AIX. Vous devez exécuter la commande **ulimit -d 524000** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **524000**.

Installation d'agents

Vous pouvez installer toute combinaison des agents de surveillance sur un système géré. Par exemple, si vous installez l'Agent Ruby pour surveiller les applications Ruby On Rails, vous souhaiterez peut-être également installer l'Agent de surveillance des temps de réponse et/ou l'Agent Linux OS. Grâce à l'Agent de surveillance des temps de réponse, vous pouvez regrouper davantage d'informations sur les temps de réponse pour vos applications Ruby. Grâce à l'Agent Linux OS, vous pouvez surveiller d'autres aspects du système, tels que l'unité centrale, la mémoire et le disque.

Pour obtenir la liste des agents qui s'exécutent sur les systèmes AIX, voir «Installation des agents sur les systèmes AIX», à la page 165.

Avant de commencer

Téléchargez les agents. Voir Chapitre 6, «Instructions de téléchargement», à la page 115.

Lisez les informations de la section Chapitre 4, «Configuration requise», à la page 71 afin de vous assurez que vous répondez aux exigences liées aux agents que vous prévoyez d'installer.

Passez en revue les tâches de pré-installation des agents avant d'installer ces derniers. Pour les détails, voir «Préinstallation sur les systèmes AIX», à la page 165.

Important : Java Runtime est installé uniquement lorsque l'agent le requiert et il n'est pas toujours disponible. En outre, ksh n'est plus requis pour l'installation des agents et SELinux en mode d'application est pris en charge.

Avant d'installer les agents, veillez à bien configurer les images des agents avec les informations de connexion du serveur Cloud APM. Si vous avez téléchargé les images d'installation d'agent dans le même répertoire que l'image d'installation du serveur, les images d'installation d'agent sont configurées automatiquement. Sinon, suivez la procédure de «Configuration des images téléchargées», à la page 162.

Pourquoi et quand exécuter cette tâche

Vous pouvez installer des agents de surveillance en tant que superutilisateur ou utilisateur non superutilisateur. Si vous ne disposez pas des privilèges de superutilisateur et que vous souhaitez installer un agent de surveillance, vous pouvez installer l'agent en tant qu'utilisateur non superutilisateur (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 183). En outre, vous ne pouvez pas installer l'agent en tant qu'utilisateur non superutilisateur si vous êtes administrateur d'hôte et que vous ne souhaitez pas exécuter l'agent de surveillance comme superutilisateur. Le flux d'installation est le même que pour un superutilisateur.

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire. Pour plus d'informations sur la coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 872.

Procédure

1. Accédez au répertoire dans lequel se trouvent vos images d'agent ou vos modules d'extension configurés. Vérifiez que le répertoire contenant vos images d'agent ne contient pas une ancienne version du fichier d'archive.
2. Procédez à l'extraction des fichiers d'installation Agent de surveillance à l'aide de la commande suivante :

   ```
   tar -xf ./fichiers d'installation
   ```

   où *fichiers d'installation* est le nom du fichier d'installation correspondant à votre offre. Pour une liste des noms de fichier, voir «Numéros de référence», à la page 118.

   Pour plus d'informations, voir «Téléchargement depuis Passport Advantage», à la page 118.

   Le script d'installation est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple : *offre*_Agent_Install_8.1.4.0. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.
3. Exécutez le script d'installation à partir du répertoire nommé en fonction du fichier archive et de la version :

   ```
   ./installAPMAgents.sh
   ```

   Pour installer les agents en mode silencieux, voir «Installation silencieuse des agents», à la page 185. Le programme d'installation vérifie que les images des agents ont été configurées avec les paramètres de connexion au serveur Cloud APM. Si les images des agents n'ont pas été configurées, l'installation est arrêtée. Vous devez configurer les images d'agent («Configuration des images téléchargées», à la page 162) et lancer la procédure d'installation d'agent à partir de l'étape 1.

4. Indiquez si vous souhaitez installer des agents individuels, une combinaison d'agents ou tous les agents.
5. Selon que vous installez ou mettez à niveau les agents, effectuez l'une des étapes suivantes :
   - Si vous installez les agents, spécifiez un autre répertoire de base d'installation d'agent ou utilisez le répertoire par défaut applicable :
     - `/opt/ibm/apm/agent`
   - Si vous mettez à niveau les agents, entrez le répertoire d'installation de la version précédente des agents à l'invite du répertoire de base d'installation des agents.
6. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser. Après avoir saisi 1 (accepter), l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer le script d'installation.

   Remarque : Si l'installation s'arrête avec le message ci-après, vérifiez si le service du serveur est démarré (Démarrer -> Outils d'administration -> Services). S'il ne l'est pas, démarrez-le, puis exécutez à nouveau `installAPMAgents.bat`.

   ```
   This script [installAPMAgents.bat] must be run as Administrator.
   ```
7. Si vous avez installé les agents à l'aide d'un ID utilisateur non superutilisateur, vous devez mettre à jour les scripts de démarrage du système (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 183).
8. Une fois l'installation terminée et la ligne de commande disponible, vous pouvez répéter les étapes de cette procédure pour installer plus d'agents de surveillance sur le système géré.

Que faire ensuite

Configurez l'agent en fonction de vos besoins. Si votre agent de surveillance requiert des opérations de configuration comme indiqué dans Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155 ou si vous voulez consulter les paramètres par défaut, voir Chapitre 10, «Configuration de votre environnement», à la page 201.

- Si un pare-feu est activé, vérifiez que les ports utilisés par l'agent de surveillance sont ouverts et disponibles. Pour plus d'informations, voir «Ports serveur Cloud APM», à la page 86.
- Si vous avez mis à niveau un agent d'une version précédente, identifiez les éventuelles tâches de reconfiguration ou de migration à effectuer avant de vous connecter à la console Cloud APM. Pour plus d'informations sur ces tâches, voir «Mise à niveau de vos agents», à la page 975. Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Pour démarrer un agent, exécutez la commande suivante :

```
./nom-agent.sh start
```

Pour plus d'informations sur les commandes de l'agent de surveillance, y compris le *nom* à utiliser, voir «Utilisation des commandes de l'agent», à la page 213. Pour plus d'informations concernant les agents démarrés automatiquement et manuellement, voir Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155.

Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Après avoir configuré et démarré l'agent, affichez les données que l'agent collecte.

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 989.

- Si vous voulez afficher les systèmes gérés de votre domaine IBM Tivoli Monitoring dans le Tableau de bord d'Application Performance, effectuez les tâches décrites dans «Intégration à IBM Tivoli Monitoring V6.3», à la page 871.

Installation des agents sur les systèmes Linux

Installez les agents de surveillance sur vos systèmes Linux pour les ressources que vous souhaitez gérer.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for MQ Appliance
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss
- Monitoring Agent for Linux OS
- Monitoring Agent for Linux KVM
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Node.js
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PHP
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for Ruby
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Synthetic Playback
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere Infrastructure Manager

- Monitoring Agent for WebSphere MQ
- Agent de surveillance des temps de réponse

Les agents suivants sont pris en charge sous Linux sur les systèmes Power Little Endian (pLinux LE) :
- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Monitoring Agent for Tomcat - La prise en charge est disponible pour la surveillance des ressources.
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Les agents suivants sont pris en charge sur les systèmes Linux for System z :
- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server - Le suivi des transactions n'est pas pris en charge.
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Agent de surveillance des temps de réponse
- Monitoring Agent for Tomcat
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

L'agent suivant est pris en charge sur les systèmes Linux for System x :
- Monitoring Agent for HTTP Server - Le suivi des transactions n'est pas pris en charge.

Préinstallation sur les systèmes Linux

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes Linux. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter aux exigences identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Installation en tant qu'utilisateur non superutilisateur
Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation. Autrement, l'installation est annulée. Pour plus d'informations sur l'installation en tant qu'utilisateur non superutilisateur, voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 183.

Limitation à 70 caractères pour le chemin d'installation
Le répertoire d'installation et son chemin d'accès ne doivent pas comporter plus de 70 caractères.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

agent DataPower

Vous devez exécuter la commande **ulimit -d unlimited** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **unlimited**. Cet agent ne peut pas être installé sur la même machine que le dispositif DataPower à surveiller.

Agent DataStage

1. Activez les paramètres dans le fichier `DSODBConfig.cfg`. Effectuez les opérations suivantes :
   a. Ouvrez le fichier `DSODBConfig.cfg` dans un éditeur à la ligne suivante :

      ```
      infosphere_information_server_install_dir/Server/DSODB
      ```

   b. Supprimez la mise en commentaire des paramètres suivants en supprimant le symbole # :

      MonitorLinks=1

      JobRunUsage=1

      ResourceMonitor=1

      DSODBON=1

   c. Editez les valeurs des paramètres définis sur 1.
2. Copiez le pilote JDBC de la base de données utilisée pour la configuration du référentiel de métadonnées sur l'ordinateur agent.
   a. Entrez 4 pour le pilote JDBC 4 ou ultérieur. Exemple : `db2jcc4.jar`
   b. Entrez 4 pour le pilote JDBC pour Oracle. Exemple : `ojdbc6.jar`
   c. Pilote JDBC pour MS SQL :
      - `Sqljdbc41.jar` nécessite l'environnement d'exécution Java 7 et prend en charge l'API JDBC 4.1.
      - `Sqljdbc42.jar` nécessite l'environnement d'exécution Java 8 et prend en charge l'API JDBC 4.2.

agent HTTP Server

Si vous installez cet agent en tant que superutilisateur, vous devez utiliser le même ID utilisateur pour exécuter et configurer l'agent.

Si vous installez et exécutez l'agent en tant qu'utilisateur non root, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître IBM HTTP Server. Vous pouvez utiliser le même ID utilisateur pour exécuter et configurer l'agent.

Agent Linux KVM

L'Monitoring Agent for Linux KVM est un agent multi-instance et multiconnexion qui prend en charge des connexions d'hyperviseur KVM basé sur Enterprise Linux et des environnements RHEVM (Red Hat Enterprise Virtualization Manager). Vous pouvez créer plusieurs instances de cet agent pour surveiller plusieurs hyperviseurs dans un environnement d'hyperviseur RHEV-M ou KVM. Vous pouvez surveiller les charges de travail virtualisées et analyser la capacité de ressources sur des machines virtuelles différentes. Pour connecter l'agent à une machine virtuelle dans l'environnement de l'hyperviseur KVM, vous devez installer les conditions préalables requises : `libvirt*.rpm` et interpréteur de commandes Korn (pdksh). L'agent collecte des indicateurs en se connectant à distance à un hyperviseur libvirt qui gère les machines virtuelles.

Agent MongoDB

Vous devez installer et configurer l'Agent MongoDB sur le système sur lequel le serveur de base de données MongoDB est installé.

Agent MySQL

Pour surveiller un environnement MySQL, le serveur MySQL et le pilote MySQL JDBC doivent être installés avant d'installer l'Monitoring Agent for MySQL. Par exemple, pour installer le pilote JDBC sur Red Hat Enterprise Linux, utilisez la commande suivante :

```
yum install mysql-connector-java
```

Une fois que vous avez démarré l'installation de l'agent et au cours du contrôle des prérequis du nom de package MySQL, un avertissement peut être affiché si un fournisseur autre que Red Hat, tel qu'Oracle, est utilisé. Si MySQL Server et le pilote JDBC sont disponibles, cet avertissement n'entraîne pas l'échec de l'installation et vous pouvez ignorer le message. Exemple de sortie :

```
Scenario: Prerequisite Scan
KSE - Monitoring Agent for MySQL Prerequisite Checker [version 01000005]:
Property                              Result   Found                                    Expected
========                      ====== =====       ========
os.package.mysql-server         WARN  Unavailable  mysql-server-5.1.12+
os.package.mysql-connector-java WARN Unavailable mysql-connector-java-5.
1.12+
```

Agent Node.js

La version de Node.js que vous utilisez pour exécuter l'application surveillée doit être identique à la version installée par défaut.

Node.js v5 n'est actuellement pas pris en charge.

Agent OpenStack

Avant de pouvoir utiliser l'Agent OpenStack vous devez avoir les logiciels suivants sur le serveur où vous installez l'agent :

- Python 2.6.0, Python 2.7.0 ou une version ultérieure
- Clients OpenStack les plus récents :
  - OpenStack
  - Keystone
  - Neutron
  - Swift

  Pour installer les clients de ligne de commande OpenStack, voir Install the OpenStack command-line clients.
- Bibliothèque Paramiko pour l'accès à distance dans Python.

  Remarque : Si vous souhaitez installer l'Agent OpenStack sur un serveur RedHat Linux nettoyé, avant d'installer la bibliothèque Paramiko, exécutez la commande suivante pour installer le logiciel requis :

  ```
  wget https://ftp.dlitz.net/pub/dlitz/crypto/pycrypto/pycrypto-2.6.1.tar.gz
  yum install gcc/openssl-devel/libffi-devel
  ```
- Interpréteur de commandes Korn

Agent Oracle Database

Sous Red Hat Enterprise Linux version 5 et version 6 et SUSE Linux Enterprise Server version 11 et version 12 x64, si l'Agent Oracle Database surveille la base de données Oracle à distance, vous devez commencer par installer les clients Oracle Instant. Installez les clients Oracle Instant à partir de la page Téléchargements Oracle Technology Network - Instant Client.

Les clients Instant v10.x ,v11.x et v12.x sont pris en charge par l'Agent Oracle Database.

Agent PHP

Si l'application PHP est déployée à l'aide du superutilisateur, vous devez utiliser ce dernier pour installer, configurer, démarrer ou arrêter l'agent. Si l'application PHP est déployée à l'aide d'un utilisateur non superutilisateur, vous pouvez utiliser le superutilisateur ou le même utilisateur non superutilisateur pour installer, configurer, démarrer ou arrêter l'agent.

Une application WordPress existante doit être installée. L'Agent PHP surveille WordPress version 3.7.1 ou ultérieure.

L'agent évalue uniquement les performances des requêtes PHP dans les applications WordPress. Le chargement CSS et JS n'est pas évalué.

L'agent n'utilise pas les arguments d'URL pour identifier les URL.

collecteur de données Python

Le collecteur de données Python surveille les applications Django.

Agent de surveillance des temps de réponse

Avant d'installer l'Agent de surveillance des temps de réponse, passez en revue la section relative à la planification de l'installation ici : «Planification de l'installation», à la page 640.

Agent SAP HANA Database

1. Installez le client de base de données SAP HANA HDBSQL version 1.00.102.06 ou ultérieure sur le système Linux.

   Important : Pour le système d'exploitation 64 bits RHEL 5.x, installez Linux SUSE 9 sur le client de base de données SAP HANA x86_64 64 bits au lieu de Linux sur x86_64 64 bits. Pour RHEL 6.x ou les systèmes d'exploitation 64 bits ultérieurs, installez Linux sur le client de base de données SAP HANA x86_64 64 bits.
2. Exécutez la commande suivante pour ajouter le chemin du répertoire d'installation à la variable d'environnement **LD_LIBRARY_PATH** :

   `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:`*`chemin_répertoire_install`*

   Exemple : `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/sap/hdbclient`, où `/usr/sap/hdbclient` indique le chemin d'installation du client de base de données SAP HANA.

Important :

Si le chemin d'installation du client de base de données SAP HANA n'est pas ajouté à la variable d'environnement **LD_LIBRARY_PATH**, le scanner de prérequis renvoie le résultat `FAIL`.

La variable d'environnement que vous avez ajoutée à l'aide de la commande export est conservée uniquement pour une session donnée du terminal. Par conséquent, assurez-vous d'avoir exécuté le script d'installation de l'agent depuis le même terminal que celui utilisé pour ajouter la variable d'environnement.

Agent Synthetic Playback

Pour installer l'Agent Synthetic Playback, l'utilisateur du système d'exploitation doit disposer des droits suivants :

- Activez le droit d'accès en lecture et exécution à l'image d'installation.
- Activez le droit d'accès en écriture à l'agent principal.

Pour exécuter l'Agent Synthetic Playback, l'utilisateur du système d'exploitation doit disposer des droits suivants :

- Activez le droit d'accès en lecture, écriture et exécution à l'emplacement d'installation de l'agent et à ses sous-répertoires et fichiers.
- Activez le droit d'exécution de Mozilla Firefox.
- Assurez-vous que les fichiers binaires d'exécution de Mozilla Firefox se trouvent dans la variable d'environnement PATH du profil de l'utilisateur.

Avant d'installer l'Agent Synthetic Playback, procédez comme suit :

1. Synchronisez les emplacements d'installation de l'agent avec la console Cloud APM.
2. Installez Mozilla Firefox et le serveur d'affichage Xvfb.
3. Vérifiez que le serveur d'affichage Xvfb fonctionne. Exécutez la commande suivante :

   ```
   # Xvfb -ac
   ```

   Aucune erreur ne devrait apparaître dans la sortie.
4. Vérifiez que le processus Xvfb est en cours. Exécutez la commande suivante :

   ```
   # ps -ef|grep Xvfb
   ```

Exemple de sortie :

```
root 7192 1 0 Jan14 ? 00:00:14 Xvfb -ac
root 20393 17900 0 02:05 pts/0 00:00:00 grep -i xvfb
```

5. Arrêtez le processus Xvfb. Exécutez la commande suivante :

   ```
   # kill -9 7192
   ```

6. Accédez à *rép_install*/etc/hosts et éditez le début du fichier hosts de sorte à inclure les paramètres suivants :

   ```
   127.0.0.1 localhost
   ```

   Ensuite, sauvegardez et fermez le fichier hosts.

Agent WebSphere Applications

Avant l'installation de l'agent, le programme de vérification des prérequis vérifie que le paramètre *ulimit* est défini sur **524000** sur le système Linux. Vous devez exécuter la commande **ulimit -d 524000** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **524000**.

Installation d'agents

Vous pouvez installer toute combinaison des agents de surveillance sur un système géré. Par exemple, si vous installez l'Agent Ruby pour surveiller les applications Ruby On Rails, vous souhaiterez peut-être également installer l'Agent de surveillance des temps de réponse et/ou l'Agent Linux OS. Grâce à l'Agent de surveillance des temps de réponse, vous pouvez regrouper davantage d'informations sur les temps de réponse pour vos applications Ruby. Grâce à l'Agent Linux OS, vous pouvez surveiller d'autres aspects du système, tels que l'unité centrale, la mémoire et le disque.

Pour obtenir la liste des agents qui s'exécutent sur les systèmes Linux, voir «Installation des agents sur les systèmes Linux», à la page 170.

Avant de commencer

Téléchargez les agents. Voir Chapitre 6, «Instructions de téléchargement», à la page 115.

Lisez les informations de la section Chapitre 4, «Configuration requise», à la page 71 afin de vous assurez que vous répondez aux exigences liées aux agents que vous prévoyez d'installer.

Passez en revue les tâches de pré-installation des agents avant d'installer ces derniers. Pour les détails, voir «Préinstallation sur les systèmes Linux», à la page 171.

Remarque : Java Runtime est installé uniquement lorsque l'agent le requiert et il n'est pas toujours disponible. En outre, ksh n'est plus nécessaire dans le cadre de l'installation des agents, sauf en ce qui concerne l'Agent Summarization and Pruning, qui est installé lors de l'installation du serveur Cloud APM. SELinux en mode d'application n'est pas pris en charge.

Avant d'installer les agents, veillez à bien configurer les images des agents avec les informations de connexion du serveur Cloud APM. Si vous avez téléchargé les images d'installation d'agent dans le même répertoire que l'image d'installation du serveur, les images d'installation d'agent sont configurées automatiquement. Sinon, suivez la procédure de «Configuration des images téléchargées», à la page 162.

Pourquoi et quand exécuter cette tâche

Vous pouvez installer des agents de surveillance en tant que superutilisateur ou utilisateur non superutilisateur. Si vous ne disposez pas des privilèges de superutilisateur et que vous souhaitez installer un agent de surveillance, vous pouvez installer l'agent en tant que utilisateur non superutilisateur (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 183). En outre, vous ne

pouvez pas installer l'agent comme utilisateur non superutilisateur si vous êtes administrateur d'hôte et que vous ne souhaitez pas exécuter l'agent de surveillance comme superutilisateur. Le flux d'installation est le même que pour un superutilisateur.

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire. Pour plus d'informations sur la coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 872.

Procédure

1. Accédez au répertoire dans lequel se trouvent vos images d'agent ou vos modules d'extension configurés. Vérifiez que le répertoire contenant vos images d'agent ne contient pas une ancienne version du fichier d'archive.
2. Extrayez les fichiers d'installation de l'Agent de surveillance en utilisant les commandes suivantes, qui dépendent de votre offre :

   ```
   tar -xf ./fichiers d'installation.tar
   ```

   où *fichiers d'installation* est le nom du fichier d'installation correspondant à votre offre. Pour une liste des noms de fichier, voir «Numéros de référence», à la page 118.

   Pour plus d'informations, voir «Téléchargement depuis Passport Advantage», à la page 118.

   Le script d'installation est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple : *offre*_Agent_Install_8.1.4. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.
3. Exécutez le script d'installation à partir du répertoire nommé en fonction du fichier archive et de la version :

   ```
   ./installAPMAgents.sh
   ```

   Pour installer les agents en mode silencieux, voir «Installation silencieuse des agents», à la page 185. Le programme d'installation vérifie que les images des agents ont été configurées avec les paramètres de connexion au serveur Cloud APM. Si les images des agents n'ont pas été configurées, l'installation est arrêtée. Vous devez configurer les images d'agent («Configuration des images téléchargées», à la page 162) et lancer la procédure d'installation d'agent à partir de l'étape 1.
4. Indiquez si vous souhaitez installer des agents individuels, une combinaison d'agents ou tous les agents.
5. Selon que vous installez ou mettez à niveau les agents, effectuez l'une des étapes suivantes :
   - Si vous installez les agents, spécifiez un autre répertoire de base d'installation d'agent ou utilisez le répertoire par défaut applicable :
     - `/opt/ibm/apm/agent`
   - Si vous mettez à niveau les agents, entrez le répertoire d'installation de la version précédente des agents à l'invite du répertoire de base d'installation des agents.
6. Lorsque vous êtes invité à accepter le contrat de licence, entrez `1` pour l'accepter et continuer ou `2` pour refuser. Après avoir saisi 1 (accepter), l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer le script d'installation.

   Remarque : Si l'installation s'arrête avec le message ci-après, vérifiez si le service du serveur est démarré (Démarrer -> Outils d'administration -> Services). S'il ne l'est pas, démarrez-le, puis exécutez à nouveau `installAPMAgents.bat`.

   ```
   This script [installAPMAgents.bat] must be run as Administrator.
   ```

7. Si vous avez installé les agents à l'aide d'un ID utilisateur non superutilisateur, vous devez mettre à jour les scripts de démarrage du système (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 183).
8. Une fois l'installation terminée et la ligne de commande disponible, vous pouvez répéter les étapes de cette procédure pour installer plus d'agents de surveillance sur le système géré.

Que faire ensuite

Configurez l'agent en fonction de vos besoins. Si votre agent de surveillance requiert des opérations de configuration comme indiqué dans Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155 ou si vous voulez consulter les paramètres par défaut, voir Chapitre 10, «Configuration de votre environnement», à la page 201.

- Si un pare-feu est activé, vérifiez que les ports utilisés par l'agent de surveillance sont ouverts et disponibles. Pour plus d'informations, voir «Ports serveur Cloud APM», à la page 86.
- Si vous avez mis à niveau un agent d'une version précédente, identifiez les éventuelles tâches de reconfiguration ou de migration à effectuer avant de vous connecter à la console Cloud APM. Pour plus d'informations sur ces tâches, voir «Mise à niveau de vos agents», à la page 975. Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Pour démarrer un agent, exécutez la commande suivante :

```
./nom-agent.sh start
```

Pour plus d'informations sur les commandes relatives aux agents de surveillance, y compris le nom à utiliser, voir «Utilisation des commandes de l'agent», à la page 213. Pour plus d'informations concernant les agents démarrés automatiquement et manuellement, voir Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155.

Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Après avoir configuré et démarré l'agent, affichez les données que l'agent collecte.

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 989.
- Si vous voulez afficher les systèmes gérés de votre domaine IBM Tivoli Monitoring dans le Tableau de bord d'Application Performance, effectuez les tâches décrites dans «Intégration à IBM Tivoli Monitoring V6.3», à la page 871.

Installation des agents sur les systèmes Windows

Vous pouvez installer des agents de surveillance Cloud APM sur des systèmes Windows.

Les agents de surveillance suivants sont pris en charge sur les systèmes Windows 64 bits. Lorsque cela est indiqué, les agents sont également pris en charge sur les systèmes Windows de 32 bits.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop

- Monitoring Agent for HTTP Server*
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for MQ Appliance
- Monitoring Agent for JBoss
- Monitoring Agent for Microsoft Active Directory*
- Monitoring Agent for Microsoft Cluster Server*
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Hyper-V Server
- Monitoring Agent for Microsoft Internet Information Services*
- Monitoring Agent for Skype for Business Server (anciennement Microsoft Lync Server)*
- Monitoring Agent for Microsoft .NET
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Microsoft SharePoint Server
- Monitoring Agent for Microsoft SQL Server*
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS*
- Agent de surveillance des temps de réponse*
- Internet Service Monitoring n'est pris en charge que sur les systèmes Windows 32 bits.

* Pris en charge sur les systèmes Windows 64 et 32 bits.

Préinstallation sur les systèmes Windows

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes Windows. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter aux exigences identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Installation à partir de l'invite de commande sur une unité locale
Utilisez l'invite de commande Windows pour lancer le script d'installation. N'utilisez pas Windows PowerShell pour lancer le script d'installation.

Copiez les fichiers d'installation sur un disque local ou une unité réseau mappée et lancez ensuite le script d'installation. Ne lancez pas ce dernier à partir d'un emplacement réseau.

Lancez le script d'installation à partir d'une nouvelle invite de commande. Ne lancez pas le script d'installation à partir d'une invite de commande existante car cette dernière peut comporter des variables d'environnement périmées.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

Agent DataStage

1. Activez les paramètres dans le fichier `DSODBConfig.cfg`. Effectuez les opérations suivantes :
   a. Ouvrez le fichier `DSODBConfig.cfg` dans un éditeur à la ligne suivante :
      ```
      infosphere_information_server_install_dir\Server\DSODB
      ```
   b. Supprimez la mise en commentaire des paramètres suivants en supprimant le symbole # :
      ```
      MonitorLinks=1
      JobRunUsage=1
      ResourceMonitor=1
      DSODBON=1
      ```
   c. Editez les valeurs des paramètres définis sur 1.
2. Copiez le pilote JDBC de la base de données utilisée pour la configuration du référentiel de métadonnées sur l'ordinateur agent.
   a. Entrez 4 pour le pilote JDBC 4 ou ultérieur. Exemple : `db2jcc4.jar`
   b. Entrez 4 pour le pilote JDBC pour Oracle. Exemple : `ojdbc6.jar`
   c. Pilote JDBC pour MS SQL :
      - `Sqljdbc41.jar` nécessite l'environnement d'exécution Java 7 et prend en charge l'API JDBC 4.1.
      - `Sqljdbc42.jar` nécessite l'environnement d'exécution Java 8 et prend en charge l'API JDBC 4.2.

Internet Service Monitoring
Pour Internet Service Monitoring, vous devez appliquer IBM Cloud Application Performance Management 8.1.4.0 Core Framework Interim Fix 3 sur APM Server à partir d'ici, puis préconfigurer l'agent. L'agent et le module de pont utilisent les ports 9510 et 9520. Au cas où ces ports sont déjà utilisés, l'installation est suspendue.

Agent MySQL
Pour l'Monitoring Agent for MySQL, vous devez installer le serveur MySQL et le pilote JDBC MySQL avant d'installer l'Agent MySQL sur ce système. Pour installer le pilote JDBC, voir Pilote MySQL Connector/J JDBC.

Si vous installez l'agent sur une machine virtuelle que vous envisagez d'utiliser comme image de bibliothèque de base, ne configurez pas l'Agent MySQL avant d'avoir instancié les autres machines virtuelles. L'Agent MySQL doit être configuré sur chaque machine virtuelle instanciée.

Agent Oracle Database

Si l'Agent Oracle Database surveille la base de données Oracle à distance, vous devez au préalable installer les clients Oracle Instant depuis Téléchargements Oracle Technology Network - Instant Client sur les systèmes suivants :

- Windows Server 2012 64 bits
- Windows Server 2012 R2 64 bits
- Windows Server 2008 R2 Datacenter 64 bits
- Windows Server 2008 R2 Enterprise 64-bits
- Windows Server 2008 R2 Standard 64 bits

Les clients Instant v10.x ,v11.x et v12.x sont pris en charge par l'Agent Oracle Database.

Agent de surveillance des temps de réponse

Avant d'installer l'Agent de surveillance des temps de réponse, passez en revue la section relative à la planification de l'installation ici : «Planification de l'installation», à la page 640.

Agent SAP HANA Database

1. Installez le client de base de données SAP HANA HDBSQL version 1.00.102.06 ou ultérieure sur le système Windows.
2. Ajoutez le chemin d'accès du client SAP HANA à la variable d'environnement **PATH**.

   Exemple : Ajoutez `C:\Program Files\sap\hdbclient` à la variable d'environnement **PATH**, où `C:\Program Files\sap\hdbclient` indique le chemin d'accès du client de base de données SAP HANA.

Agent Tomcat

1. Le kit SDK Java est installé sur le serveur Tomcat sur lequel l'agent est installé.
2. Le chemin d'accès au kit SDK est ajouté à la variable *PATH* directement, ou à l'aide de la commande **set path** avant d'installer l'agent.
3. La commande **JAR** fonctionne.

Installation d'agents

Vous pouvez installer toute combinaison des agents de surveillance sur un système géré. Par exemple, si vous installez l'Monitoring Agent for MySQL pour surveiller des serveurs MySQL, vous pouvez également installer l'Agent de surveillance des temps de réponse afin de collecter plus d'informations sur les temps de réponse de vos applications Ruby. Vous pouvez également installer l'Monitoring Agent for Windows OS pour surveiller d'autres aspects du système, tels que l'unité centrale globale, la mémoire et le disque.

Votre offre détermine les agents de surveillance disponibles pour l'installation. Pour obtenir la liste des agents compris dans chaque offre, voir «Fonctions», à la page 40.

Pour obtenir la liste des agents qui s'exécutent sur un système Windows, voir «Préinstallation sur les systèmes Windows», à la page 178.

Avant de commencer

Téléchargez les agents. Voir Chapitre 6, «Instructions de téléchargement», à la page 115.

Lisez les informations de la section Chapitre 4, «Configuration requise», à la page 71 afin de vous assurez que vous répondez aux exigences liées aux agents que vous prévoyez d'installer.

Revoyez les tâches prérequises des agents avant d'installer ces derniers. Pour plus de détails, voir «Préinstallation sur les systèmes Windows», à la page 178.

Avant d'installer les agents, vous devez configurer les images des agents avec les informations de connexion du serveur Cloud APM. Si vous avez téléchargé les images d'installation d'agent dans le même répertoire que l'image d'installation du serveur, les images d'installation d'agent sont configurées automatiquement. Sinon, suivez la procédure de «Configuration des images téléchargées», à la page 162.

Pourquoi et quand exécuter cette tâche

Vérifiez que vous disposez des droits appropriés pour exécuter le script d'installation de l'agent et les commandes d'agent. Vous devez être connecté à l'aide de l'un des types de compte utilisateur suivants :

- Compte utilisateur administrateur Windows par défaut
- Compte utilisateur administrateur
- Compte utilisateur membre du groupe Administrateurs
- Compte utilisateur enregistré en tant qu'administrateur dans les services Active Directory

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire. Pour plus d'informations sur la coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 872.

Procédure

Pour installer des agents de surveillance sur des machines virtuelles et des systèmes sur lesquels le système d'exploitation Windows est installé, procédez comme suit :

1. Sur votre système, accédez au répertoire qui contient les images d'agent configurées.
2. Procédez à l'extraction des fichiers d'installation de l'agent associés à votre offre (ou à vos offres) à l'emplacement où vous voulez installer le logiciel d'agent de surveillance. Pour une liste des noms de fichier, voir «Numéros de référence», à la page 118.

   Pour plus d'informations, voir «Téléchargement depuis Passport Advantage», à la page 118 Le script d'installation .bat est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple : *offre*_Agent_Install_8.1.4.0. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.
3. Ouvrez une invite de commande en tant qu'administrateur.
   a. Dans le menu **Démarrer**, tapez `commande` dans la zone de recherche.
   b. Cliquez sur **Invite de commandes** avec le bouton droit de la souris dans la liste qui s'affiche, puis sélectionnez **Exécuter en tant qu'administrateur**.
4. A partir de l'invite de commande, exécutez le script d'installation avec des privilèges d'administrateur à partir du répertoire nommé en fonction du fichier archive et de la version :

   ```
   cd offre_Agent_Install_version
   installAPMAgents.bat
   ```

   Le programme d'installation vérifie que les images des agents ont été configurées avec les paramètres de connexion au serveur Cloud APM. Si les images des agents n'ont pas été configurées, l'installation est arrêtée. Vous devez configurer les images d'agent («Configuration des images téléchargées», à la page 162) et lancer la procédure d'installation d'agent à partir de l'étape 1.

   Restriction : Pour l'Agent WebSphere Applications, les privilèges d'administration doivent être les mêmes que ceux utilisés pour installer WebSphere Application Server.
   Pour installer les agents en mode silencieux, voir «Installation silencieuse des agents», à la page 185.
5. Si vous installez les agents, indiquez le nom du répertoire d'installation. Le chemin d'installation par défaut est `C:\IBM\APM`. Le nom du répertoire d'installation ne doit pas comporter plus de 80 caractères ni contenir des caractères non ASCII, spéciaux ou codés sur deux octets. Les noms de répertoire dans

le chemin doivent contenir uniquement les caractères suivants :
`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ _\:0123456789()~-./.`

Remarque : Lorsque la création de noms de fichier courts (*8dot3Name*) est désactivée, si les noms de répertoire dans le chemin d'accès contiennent des espaces, l'installation n'est pas prise en charge.

Si vous mettez à niveau l'agent, cette étape est ignorée et l'agent est installé dans le répertoire d'installation précédent.

6. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser. Après avoir saisi 1 (accepter), l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer le script d'installation.

   Remarque : Si l'installation s'arrête avec le message ci-après, vérifiez si le service du serveur est démarré (Démarrer -> Outils d'administration -> Services). S'il ne l'est pas, démarrez-le, puis exécutez à nouveau `installAPMAgents.bat`.

   ```
   This script [installAPMAgents.bat] must be run as Administrator.
   ```

7. Une fois l'installation terminée et la ligne de commande disponible, répétez ces étapes pour installer d'autres agents de surveillance.

Que faire ensuite

Configurez vos agents en fonction de vos besoins. Pour vérifier si votre agent de surveillance requiert une configuration manuelle, voir Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155. Pour des instructions de configuration, ou si vous souhaitez passer en revue les paramètres de configuration par défaut, voir Chapitre 10, «Configuration de votre environnement», à la page 201.

Avant d'installer de nouveaux agents, le programme d'installation de Windows arrête temporairement tous les agents en cours d'exécution à l'emplacement du produit installé. Une fois l'installation terminée, le programme d'installation redémarre tous les agents arrêtés. Vous devez redémarrer manuellement tout agent de surveillance que le programme d'installation ne démarre pas automatiquement.

- Si un pare-feu est activé, vérifiez que les ports utilisés par l'agent de surveillance sont ouverts et disponibles. Pour plus d'informations, voir «Ports serveur Cloud APM», à la page 86.
- Si vous avez mis à niveau un agent d'une version précédente, identifiez les tâches de reconfiguration ou de migration à effectuer avant de vous connecter à la console Cloud APM. Pour plus d'informations sur ces tâches, voir «Mise à niveau de vos agents», à la page 975.

Utilisez l'une des méthodes suivantes pour démarrer l'agent :

- Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**. Cliquez avec le bouton droit de la souris sur un agent et cliquez sur **Start**.
- Exécutez la commande suivante :

  ```
  nom-agent.bat start
  ```

Pour plus d'informations sur les commandes relatives aux agents de surveillance, y compris le nom à utiliser, voir «Utilisation des commandes de l'agent», à la page 213. Pour plus d'informations sur les agents démarrés automatiquement et manuellement, voir Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155.

Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Après avoir configuré et démarré l'agent, affichez les données que l'agent collecte.

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 989.
- Si vous voulez afficher les systèmes gérés de votre domaine IBM Tivoli Monitoring dans le Tableau de bord d'Application Performance, effectuez les tâches décrites dans «Intégration à IBM Tivoli Monitoring V6.3», à la page 871.

Installation des agents en tant qu'utilisateur non superutilisateur

Si vous ne disposez pas des privilèges superutilisateur et que vous souhaitez installer un agent de surveillance, vous pouvez installer l'agent comme un utilisateur non-superutilisateur. En outre, vous ne pouvez pas installer l'agent comme utilisateur non-superutilisateur si vous êtes administrateur d'hôte et que vous ne souhaitez pas exécuter l'agent de surveillance comme superutilisateur. Le flux d'installation est le même que pour un superutilisateur. Après une installation non superutilisateur, exécutez le script **UpdateAutoRun.sh** avec des droits d'accès de superutilisateur ou d'utilisateur sudo.

Avant de commencer

Pour identifier le système informatique de manière unique, l'Agent Linux OS doit identifier l'identificateur unique universel (UUID), le fabricant, le modèle et le numéro de série de la carte mère du système informatique. Ces informations sont obligatoires pour que l'agent puisse être ajouté à une application dans la console Cloud APM.

Pour obtenir les informations sur le système informatique, procédez comme suit :

1. Assurez-vous que la commande **/usr/bin/hal-get-property** est installée sur le système informatique et que le processus hald (démon HAL) est en cours d'exécution.
2. Si la commande **/usr/bin/hal-get-property** n'est pas installée sur le système informatique, confirmez que le fichier `/sys/class/dmi/id/product_uuid` existe et qu'il contient l'identificateur unique universel du système informatique.

Remarque : L'Agent Linux OS récupère ces informations régulièrement de telle sorte que les commandes ou les fichiers mentionnés aux étapes précédentes doivent rester aux mêmes emplacements, même après l'installation.

Procédure

1. Installez vos agents de surveillance sous Linux ou AIX, comme décrit dans les rubriques «Installation des agents sur les systèmes Linux», à la page 170 et «Installation des agents sur les systèmes AIX», à la page 165.
2. Facultatif : Si vous avez installé votre agent avec un utilisateur sélectionné et que vous souhaitez configurer l'agent avec un autre utilisateur, exécutez le script `./secure.sh`. Pour plus d'informations sur le script **./secure.sh**, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 219 et Sécurisation des fichiers d'installation de l'agent. Par exemple : **./secure.sh -g db2iadm1**
3. Facultatif : Au besoin, configurez vos agents de surveillance sous Linux ou AIX (voir Chapitre 10, «Configuration de votre environnement», à la page 201).
4. Pour mettre à jour les scripts de démarrage du système, exécutez le script suivant avec des droits d'accès de superutilisateur ou d'utilisateur sudo: *rép_install*`/bin/UpdateAutoRun.sh`

Que faire ensuite

Si vous avez installé votre agent en tant qu'utilisateur superutilisateur et que vous souhaitez configurer l'agent de la même manière, aucune action spéciale n'est requise. Si vous avez installé votre agent avec un utilisateur sélectionné et que vous souhaitez le configurer avec un autre utilisateur, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 219.

Si vous avez installé et configuré votre agent en tant qu'utilisateur non superutilisateur et que vous souhaitez démarrer l'agent de la même manière, aucune action spéciale n'est requise. Si vous avez installé et configuré votre agent avec un utilisateur sélectionné et que vous souhaitez le démarrer avec un autre utilisateur, voir «Démarrage d'agents en tant qu'utilisateur non superutilisateur», à la page 1039.

Utilisez le même ID utilisateur pour l'installation et les mises à niveau des agents.

Si vous exécutez le script **UpdateAutoRun.sh** en tant que superutilisateur, l'agent est configuré de sorte à démarrer automatiquement suite au redémarrage du système d'exploitation. Si vous ne voulez pas que l'agent ait ce comportement, vous pouvez désactiver le démarrage automatique de l'agent. Pour plus d'informations, voir «Désactivation du démarrage automatique de l'agent sur les systèmes AIX et Linux», à la page 220.

Sécurisation des fichiers d'installation de l'agent

Après avoir installé les agents de surveillance sous le nom d'un utilisateur non superutilisateur sur des systèmes Linux ou AIX, vous pouvez exécuter le script `secure.sh` pour sécuriser l'installation des agents en supprimant les droits en écriture "world" et en définissant la propriété de fichier correcte.

Avant de commencer

- Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation.
- L'installation des agents de surveillance et toute configuration d'agent doivent être effectuées sur le système et les agents doivent être correctement démarrés.
- Si vous exécutez des agents en utilisant des comptes utilisateur différents, ces comptes doivent être membres du même groupe. (Voir l'option `-g`.)

Pourquoi et quand exécuter cette tâche

Effectuez cette étape pour verrouiller les droits d'accès aux fichiers dans votre installation. Des options sont disponibles pour qu'aucun mot de passe root ne soit requis, pour spécifier un nom de groupe et pour afficher l'aide de la commande.

Procédure

Exécutez la commande suivante à partir du répertoire *rép_install*`/bin`. Syntaxe :

```
secure.sh [-g common_group] [-n] [-h]
```

- Dans le mode le plus simple, exécutez le script **`./secure.sh`** qui supprime les droits "world" et définit l'utilisateur en cours et le groupe de l'utilisateur comme propriétaires du fichier. Si le script est exécuté par un utilisateur non superutilisateur, le système demande le mot de passe root.
- Si un utilisateur non superutilisateur exécute le script **`./secure.sh`** avec l'option `-n`, le système ne demande pas le mot de passe root. Dans ce cas, vous changez les droits de fichier et la propriété en utilisant les privilèges de l'utilisateur. Si le répertoire d'installation contient des fichiers détenus par des utilisateurs différents et que l'utilisateur n'a pas de privilèges pour modifier les autorisations et la propriété des fichiers des autres utilisateurs, ce mode échoue.
- Si vous voulez définir un groupe comme propriétaire de groupe, le propriétaire doit fournir l'option `-g` avec un nom de groupe valide comme argument pour l'option. (Voir Exemple.)
  Lancez `secure.sh -g` *groupe_commun*.
  Cette commande modifie la propriété des fichiers et des répertoires de manière récursive.

  Si le groupe *groupe_commun* n'est pas le groupe principal de l'utilisateur, vous pouvez le définir comme étant le propriétaire de groupe des nouveaux fichiers créés dans un répertoire, en exécutant la commande suivante :

  ```
  chmod g+s rép_install/bin/sous_rép
  ```

  où, *sous_rép* est un sous-répertoire, par exemple `/opt/ibm/ccm/agent`.

- Exécutez le script **./secure.sh** avec l'option –h pour obtenir l'aide relative au script.

Résultats

Le répertoire d'installation n'autorise l'accès qu'à l'utilisateur ayant exécuté le script ou aux utilisateurs du groupe spécifié.

Exemple

Si l'utilisateur Alice est membre du groupe système «apmgroup», il peut utiliser ce groupe pour définir la propriété du groupe de fichiers à l'aide de la commande suivante :

```
./secure.sh -g apmgroup
```

Une fois que le script a été exécuté, le groupe est défini sur «apmgroup» pour tous les fichiers du répertoire *rép_install* pour le groupe.

Que faire ensuite

L'exécution du script **./secure.sh** doit définir les droits d'accès suivants pour les agents.

```
rwx rwx ---
```

Après avoir exécuté le script, vérifiez les droits d'accès pour les fichiers d'agent. Par exemple, pour la surveillance des temps de réponse, vérifiez les fichiers dans *rép_install*/*arch*/hu/lib/mod_wrt.so. Si les droits d'accès pour ces fichiers ne sont pas correctement définis, mettez-les à jour manuellement. Par exemple, pour l'agent de surveillance des temps de réponse :

1. Définissez les droits d'accès, exécutez :

   ```
   chmod g+rx $AGENT_HOME/bin/rt-agent.sh
   ```

2. Définissez l'utilisateur et le groupe, exécutez :

   ```
   chown nouvel_utilisateur:nouveau_groupe $AGENT_HOME/bin/rt-agent.sh
   ```

Installation silencieuse des agents

L'installation des agents en mode silencieux réduit la durée d'installation. Pour installer un agent de surveillance en mode silencieux, vous devez télécharger le fichier d'archive des images d'installation de cet agent à partir du site de téléchargement d'IBM, préconfigurer les images de l'agentsite Web, extraire les fichiers d'installation de l'agent, préparer un fichier de réponses silencieux et exécuter le script d'installation en mode silencieux.

Avant de commencer

1. Consultez les tâches prérequises pour l'installation des agents de surveillance, puis téléchargez et extrayez les fichiers d'installation des agents. Pour plus de détails, voir Installation des agents sur les systèmes AIX, Installation des agents sur les systèmes Linux ou Installation des agents sur les systèmes Windows.
2. Pour préparer un fichier de réponses silencieux pour l'installation des agents, procédez comme suit :
   a. Recherchez le fichier d'installation silencieux pour votre ou vos offres *offre*_silent_install.txt, créez-en une copie et ouvrez-le dans un éditeur de texte.
   b. Supprimez la mise en commentaire du contrat de licence.
   c. Pour spécifier les agents que vous voulez installer, effectuez l'une des étapes suivantes :
      - Supprimez la mise en commentaire des agents individuels à installer. Par exemple :

        ```
        INSTALL_AGENT=os
        INSTALL_AGENT=ruby
        ```

      - Supprimez la mise en commentaire de INSTALL_AGENT=all pour installer tous les agents.

d. Supprimez la mise en commentaire de AGENT_HOME et spécifiez le répertoire dans lequel vous voulez installer les agents.
e. Sauvegardez le fichier.

Procédure

1. Sur la ligne de commande, basculez vers le répertoire dans lequel vous avez extrait le script d'installation et exécutez la commande suivante :
   ```
   cd offre_Agent_Install_version
   ```
2. Exécutez la commande d'installation :
   - Linux AIX
     ```
     ./installAPMAgents.sh -p chemin_d'accès_au_fichier_réponses_silencieux
     ```
   - Windows
     ```
     installAPMAgents.bat -p chemin_d'accès_au_fichier_réponses_silencieux
     ```

     L'installation des agents échoue sous Windows si le scanner de prérequis ne parvient pas à obtenir le type de disque sur lequel l'agent sera installé. Si cela se produit, un résultat d'échec apparaît pour la propriété validDestLocation dans le fichier journal de l'installation. Pour contourner ce problème, ajoutez ce qui suit à la commande d'installation : SKIP_PRECHECK=1. Par exemple,
     ```
     installAPMAgents.bat -p chemin_d'accès_au_fichier_réponses_silencieux SKIP_PRECHECK=1
     ```

     Remarque : Windows Lorsque la création de noms de fichier courts (*8dot3Name*) est désactivée, si les noms de répertoire dans le chemin d'accès contiennent des espaces, l'installation n'est pas prise en charge.

Résultats

Les agents sont installés.

Que faire ensuite

Configurez les agents. Reportez-vous à la procédure et au tableau de commandes pour les systèmes Linux et AIX et les systèmes Windows.

Contournement de l'analyse des prérequis

Lorsque vous installez vos agents de surveillance, l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec.

Dans un environnement où des images de machine virtuelle servent de modèles, l'analyse des prérequis effectuée avant que l'installation ne commence ne peut être effectuée que sur la première image de modèle. Si une image de machine virtuelle réussit l'analyse, les autres machines virtuelles créées à partir de cette image le réussissent également. Vous pouvez gagner du temps en ignorant le contrôle des prérequis pour les autres machines virtuelles créées à partir de la même image.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez téléchargé et extrait les fichiers d'installation, effectuez cette étape pour ignorer l'analyse des prérequis.

Procédure

Sur le système où vous prévoyez d'installer les agents de surveillance, entrez l'une des commandes suivantes :

- Linux `export SKIP_PRECHECK=1`
- Windows `set SKIP_PRECHECK=1`

Que faire ensuite

Exécutez le script d'installation pour commencer à installer les agents de surveillance sans l'analyse des prérequis.

Désinstallation de vos agents

Désinstallez un seul agent ou tous les agents d'un système géré.

Avant de commencer

Pour les agents multi-instance, vous devez supprimer toutes les instances d'agent d'agent avant de désinstaller l'agent. Sinon, les entrées d'agent ne seront pas effacées du registre. Pour supprimer des instances, exécutez la commande suivante :

- Windows *nom*`-agent.bat remove` *nom_instance*
- Linux AIX `./`*nom*`-agent.sh remove` *nom_instance*

où, *nom* est le nom de l'agent et *nom_instance* est le nom d'instance. Pour plus d'informations, voir «Utilisation des commandes de l'agent», à la page 213. Pour une liste des agents multiple-instance, voir tableau 23, à la page 156.

Pour les agents suivants, une tâche spécifique à l'agent doit être exécutée avant de suivre la procédure de désinstallation :

- Pour l'Monitoring Agent for HTTP Server, vous devez supprimer l'instruction `Include` dans le fichier `http.conf`, par exemple, `"Include "/opt/ibm/apm/agent/tmp/khu/kvm65s2_8044.conf"`, avant de redémarrer IBM HTTP Server.
- Pour l'Monitoring Agent for Python, exécutez *rép_install*`/lx8266/pg/bin/uninstall.sh` pour supprimer les codes d'injection avant de désinstaller l'agent.
- Pour l'Monitoring Agent for PHP, exécutez *rép_install*`/bin/lx8266/pj/lib/uninstall.`*nom_instance*`.sh` pour déplacer les codes d'injection avant de désinstaller l'agent.
- Pour l'Monitoring Agent for WebSphere Applications, vous devez annuler la configuration du collecteur de données pour toutes les instances de serveur surveillées avant de désinstaller l'agent. Suivez les instructions décrites dans «Agent WebSphere Applications : Annulation de la configuration du collecteur de données», à la page 189.

  Pour l'Agent WebSphere Applications, assurez-vous que l'ID utilisateur, utilisé pour désinstaller l'agent, dispose des droits complets en lecture et en écriture sur les répertoires `logs` et `runtime` et sur tous leurs sous-répertoires et fichiers que contient le répertoire de base du collecteur de données. Le répertoire principal du collecteur de données est le suivant :
  - Windows *rép_install*`\dchome\7.3.0.14.06`
  - Linux AIX *rép_install*`/yndchome/7.3.0.14.06`
- Pour l'Agent Node.js, vous devez retirer le plug-in de surveillance de votre application Node.js avant de désinstaller l'agent. Suivez les instructions décrites dans «Agent Node.js : Retrait du plug-in de surveillance», à la page 197.
- Pour l'agent Microsoft .NET, vous devez retirer le collecteur de données de vos applications .NET avant de désinstaller l'agent. Suivez les instructions décrites dans «agent Microsoft .NET : Retrait du collecteur de données .NET», à la page 198.
- Pour l'agent IBM Integration Bus, si vous avez configuré le suivi des transactions pour des courtiers avec l'exit utilisateur fourni par l'agent, vous devez supprimer l'exit utilisateur avant de désinstaller l'agent. Suivez les instructions décrites dans «Suppression de l'exit utilisateur KQIUserExit», à la page 334.

- Pour Internet Service Monitoring, accédez à `<candle_home>\BIN` et exécutez le fichier ism-agent.bat avec `uninstall` comme argument. Si vous souhaitez désinstaller tous les agents de surveillance sur le serveur à l'aide du fichier smai-agent.bat, exécutez la commande ism-agent.bat avec l'argument `uninstall`, puis exécutez la commande smai-agent.bat

Pourquoi et quand exécuter cette tâche

L'agent Oracle sur les systèmes Windows peut être désinstallé uniquement à l'aide de l'invite de commande.

Procédure

1. Sur la machine virtuelle ou le système où l'agent ou les agents de surveillance sont installés, ouvrez une ligne de commande et accédez au répertoire des fichiers binaires :
   - Linux AIX *rép_install*`/bin`
   - Windows *rép_install*`\BIN`

   où *rép_install* est le répertoire d'installation des agents de surveillance.
2. Pour désinstaller un agent de surveillance spécifique, entrez le nom du script de l'agent et l'option de désinstallation où *nom* représente le nom du script de l'agent :
   - Linux AIX `./`*nom*`-agent.sh uninstall`
   - Windows *nom*`-agent.bat uninstall`

   Pour une liste des noms de script d'agent produit, voir «Utilisation des commandes de l'agent», à la page 213.

   A faire : Pour l'Monitoring Agent for Microsoft .NET, vous devez exécuter la commande avec des privilèges d'administrateur.

   L'agent de surveillance est désinstallé du système géré.

   Si vous avez désinstallé tous les agents de surveillance de manière individuelle, effectuez l'étape suivante pour supprimer les fichiers Framework.
3. Pour désinstaller tous les agents de surveillance du système géré avec une invite de confirmation, entrez le nom du script et l'option uninstall all :
   - Linux AIX `./smai-agent.sh uninstall_all`
   - Windows `smai-agent.bat uninstall_all`

   Une invite de confirmation s'affiche, tapez 1 pour continuer ou tapez 2 pour annuler. Tous les agents de surveillance sont désinstallés du système ou de la machine virtuelle.
4. Linux AIX Sous Linux et AIX, pour forcer la désinstallation de tous les agents de surveillance sans invite de confirmation, entrez le nom du script et l'option force uninstall all : `./smai-agent.sh uninstall_all force`

Que faire ensuite

Pour l'Monitoring Agent for HTTP Server, après l'avoir désinstallé, supprimez manuellement les fichiers suivants :

- `/tmp/khu_cps.properties`
- `/tmp/httpserver-disc.error`

Pour l'Monitoring Agent for Python :

1. Supprimez le fichier de configuration Django `pyc` afin de vous assurer que le fichier `pyc` Django génère son binaire.

2. Redémarrez le serveur Apache pour supprimer le composant middleware chargé dans les processus Apache.

Pour l'Monitoring Agent for Ruby, pour désinstaller le collecteur de données de diagnostic :

1. Accédez au répertoire principal de votre application, ouvrez son `Gemfile` et retirez la ligne suivante dans le fichier : `gem 'stacktracer'`
2. Redémarrez l'application Ruby on Rails.
3. Désinstallez le collecteur de données de diagnostic. Entrez : `gem uninstall` *`Gemfile`*
4. Retirez le répertoire d'exécution du collecteur de données. L'emplacement par défaut de ce répertoire est *`rép_install`*`/install-images/kkm/dchome`

Pour l'Monitoring Agent for Microsoft .NET, procédez comme suit :

1. Supprimez les fichiers `dll` du collecteur de données en utilisant l'une des options suivantes :
   - Réamorcez le système d'exploitation.
   - Essayez de supprimer le fichier *`rép_install`*`\qe\bin64\CorProfLog.dll`.

     Une boîte de dialogue indiquant que le fichier est en cours d'utilisation (`File in Use`) s'affiche. Elle identifie les processus .NET en cours d'exécution.
   - Redémarrez chacun des processus .NET.
2. Redémarrez vos applications .NET.

Agent WebSphere Applications : Annulation de la configuration du collecteur de données

Si vous désinstallez l'Agent WebSphere Applications avant d'avoir annulé la configuration du collecteur de données, la désinstallation de l'agent échoue. Vous pouvez supprimer le collecteur de données d'une instance de serveur d'applications de trois façons : manuellement, en recourant à l'utilitaire interactif ou bien en exécutant le processus d'annulation de la configuration en mode silencieux.

Pour la surveillance des instances avec les ressources de surveillance PMI, l'annulation de configuration est indisponible. La surveillance des données PMI se poursuit tandis que le serveur est disponible.

Annulation de la configuration interactive du collecteur de données

Si vous ne voulez plus que le collecteur de données surveille une ou plusieurs instances de serveur d'applications, vous pouvez annuler la configuration du collecteur de données pour ces instances.

Avant de commencer

Utilisez l'ID utilisateur employé pour configurer le collecteur de données pour annuler la configuration du collecteur de données ; il s'agit également de l'ID utilisateur employé pour installer le serveur d'applications. Vérifiez que cet ID utilisateur dispose de droits en lecture et en écriture sur le répertoire de base du collecteur de données et sur tous ses sous-répertoires. Le répertoire de base du collecteur de données est le suivant, où *rép_install* est le répertoire d'installation de l'Agent WebSphere Applications.

- Windows *`rép_install`*`\dchome\7.3.0.14.06`
- Linux AIX *`rép_install`*`/yndchome/7.3.0.14.06`

Pourquoi et quand exécuter cette tâche

L'utilitaire d'annulation de configuration (`unconfig.sh` ou `unconfig.bat`) est un utilitaire de ligne de commande à menus permettant d'annuler la configuration du collecteur de données.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur employé pour configurer le collecteur de données.

2. Accédez au répertoire `bin` :
   - Windows *rép_install*\dchome\7.3.0.14.06\bin
   - Linux AIX *rép_install*/yndchome/7.3.0.14.06/bin
3. Facultatif : Définissez l'emplacement du répertoire de base Java avant de démarrer l'utilitaire. Par exemple :

   Linux AIX
   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```
   Windows
   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```
4. Démarrez l'utilitaire d'annulation de configuration à l'aide de la commande suivante :

   Linux AIX
   ```
   ./unconfig.sh
   ```
   Windows
   ```
   unconfig.bat
   ```
5. L'utilitaire recherche toutes les instances de serveur qui sont surveillées par le collecteur de données. Entrez le nombre qui correspond à l'instance de serveur d'applications dont vous voulez annuler la configuration pour la collecte de données ou entrez un astérisque (`*`) pour annuler la configuration de la collecte de données pour toutes les instances de serveur d'applications. Pour indiquer un sous-ensemble de serveurs, entrez les nombres, séparés par des virgules, qui représentent les serveurs. Par exemple : `1,2,3`.

   A faire :
   - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration. (Une instance de WebSphere Application Server Liberty n'a pas besoin d'être en cours d'exécution).
   - Dans un environnement de déploiement réseau, l'agent de noeud et le gestionnaire de déploiement doivent s'exécuter.
6. L'utilitaire vous invite à indiquer si vous voulez créer une sauvegarde de votre configuration en cours de WebSphere Application Server. Entrez `1` pour créer une sauvegarde de la configuration en cours. Sinon, entrez `2` et passez à l'étape 8.
7. L'utilitaire vous invite à spécifier le répertoire dans lequel stocker la sauvegarde de la configuration. Indiquez un répertoire dans lequel stocker la sauvegarde de la configuration ou acceptez le répertoire par défaut. L'utilitaire affiche le nom du répertoire de base de WebSphere ainsi que le profil WebSphere pour lequel une sauvegarde est créée.
8. L'utilitaire indique si la sécurité globale de WebSphere est activée pour le profil WebSphere Application que vous avez indiqué. Si la sécurité globale n'est pas activée, passez à l'étape 10.
9. L'utilitaire vous invite à indiquer si les paramètres de sécurité doivent être extraits depuis un fichier de propriétés de client. Entrez `1` pour permettre à l'utilitaire d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié et passez à l'étape 10. Sinon, entrez `2` pour entrer le nom d'utilisateur et le mot de passe.

   Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP (Simple Object Access Protocol). Si la sécurité globale est activée pour un profil, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à IBM WebSphere Application Server la console d'administration pour le profil. Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI, ou le fichier `soap.client.props` pour une connexion SOAP. Si vous avez sélectionné l'option de sauvegarder la configuration en cours de WebSphere, l'utilitaire commence à sauvegarder la configuration.
10. L'utilitaire annule la configuration du collecteur de données pour les instances de serveur d'applications spécifiées. Un message d'état indique que l'annulation de la configuration du collecteur de données a abouti.

11. Une fois l'annulation de la configuration du collecteur de données terminée, redémarrez les instances du serveur d'applications. La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré. La surveillance des ressources PMI pour l'instance de serveur est toujours disponible.
12. Facultatif : Si vous souhaitez l'utiliser pour une instance de serveur après avoir annulé la configuration du collecteur de données, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
    - Windows

      ```
      cd rép_install\bin
      was-agent.bat stop
      was-agent.bat start
      ```

    - Linux AIX

      ```
      cd rép_install/bin
      ./was-agent.sh
      stop
      ./was-agent.sh start
      ```

Résultats

L'utilitaire annule la configuration du collecteur de données pour les instances de serveur d'applications spécifiées.

Annulation de la configuration du collecteur de données en mode silencieux

Vous pouvez annuler la configuration du collecteur de données à l'aide de l'utilitaire d'annulation de configuration en mode silencieux.

Avant de commencer

Utilisez l'ID utilisateur employé pour configurer le collecteur de données pour annuler la configuration du collecteur de données ; il s'agit également de l'ID utilisateur employé pour installer le serveur d'applications. Vérifiez que cet ID utilisateur dispose de droits en lecture et en écriture sur le répertoire de base du collecteur de données et sur tous ses sous-répertoires. Le répertoire de base du collecteur de données est le suivant, où *rép_install* est le répertoire d'installation de l'Agent WebSphere Applications.

- Windows *rép_install*\dchome\7.3.0.14.06
- Linux AIX *rép_install*/yndchome/7.3.0.14.06

Pourquoi et quand exécuter cette tâche

Lorsque vous annulez la configuration du collecteur de données en mode silencieux, vous indiquez d'abord des options de configuration dans un fichier de propriétés. Un exemple de fichier de propriétés, `sample_silent_unconfig.txt`, est fourni avec l'utilitaire d'annulation de configuration. Le fichier est disponible dans le répertoire `bin` au sein du répertoire de base du collecteur de données.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur employé pour configurer le collecteur de données.
2. Spécifiez les options de configuration dans le fichier `properties.txt`.

   Les propriétés suivantes peuvent être utilisées pour annuler la configuration du collecteur de données en mode silencieux :

   Paramètres de connexion de WebSphere Application Server

   was.wsadmin.connection.host
   Indique le nom de l'hôte auquel l'outil wsadmin se connecte.

Paramètres de sécurité globale de WebSphere Application Server

was.wsadmin.username
Spécifie l'ID utilisateur d'un utilisateur autorisé à se connecter à la console d'administration d'IBM WebSphere Application Server. Cet utilisateur doit posséder le rôle d'agent sur le serveur d'applications.

was.wsadmin.password
Indique le mot de passe qui correspond à l'utilisateur indiqué dans la propriété `was.wsadmin.username`.

Paramètres de WebSphere Application Server

was.appserver.profile.name
Indique le nom du profil de serveur d'applications dont vous voulez annuler la configuration.

was.appserver.home
Indique le répertoire de base de WebSphere Application Server.

was.appserver.cell.name
Indique le nom de cellule de WebSphere Application Server.

was.appserver.node.name
Indique le nom de noeud de WebSphere Application Server.

Sauvegarde de la configuration de WebSphere Application Server

was.backup.configuration
Indique si la configuration en cours du collecteur de données de WebSphere Application Server doit être ou non sauvegardée avant que vous ne procédiez à son annulation. Les valeurs valides sont `True` et `False`.

was.backup.configuration.dir
Indique l'emplacement du répertoire de sauvegarde.

Paramètres de l'instance d'exécution de WebSphere Application Server

was.appserver.server.name
Indique une instance de serveur d'applications dans le profil de serveur d'applications pour laquelle vous voulez annuler la configuration du collecteur de données.

Conseil : Le fichier de réponses silencieux peut avoir plusieurs instances de cette propriété.

3. Accédez au répertoire suivant :
   - Windows `rép_install\dchome\7.3.0.14.06\bin`
   - Linux AIX `rép_install/yndchome/7.3.0.14.06/bin`
4. Exécutez la commande suivante :
   - Windows
     `unconfig.bat -silent chemin_vers fichier_mode_silencieux`
   - Linux AIX
     `unconfig.sh -silent chemin_vers fichier_mode_silencieux`
5. Une fois l'annulation de la configuration du collecteur de données terminée, redémarrez les instances du serveur d'applications. La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré. La surveillance des ressources PMI pour l'instance de serveur est toujours disponible.
6. Facultatif : Si vous souhaitez l'utiliser pour une instance de serveur après avoir annulé la configuration du collecteur de données, redémarrez l'agent de surveillance en exécutant les commandes suivantes :

- Windows

  ```
  cd rép_install\bin
  was-agent.bat stop
  was-agent.bat start
  ```

- Linux AIX

  ```
  cd rép_install/bin
  ./was-agent.sh
  stop
  ./was-agent.sh start
  ```

Suppression manuelle de la configuration du collecteur de données depuis une instance de serveur d'applications

Pour supprimer manuellement la configuration du collecteur de données depuis une instance de serveur d'applications, vous devez pouvoir vous connecter au serveur d'applications à l'aide de l'outil wsadmin. Ce n'est possible que si vous utilisez WebSphere Application Server Network Deployment et que si Deployment Manager est en cours d'exécution. Si WebSphere Application Server ne peut pas démarrer, vous devez le restaurer à partir de la sauvegarde effectuée lors de l'exécution de l'utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous pouvez supprimer manuellement la configuration du collecteur de données d'une instance de serveur d'applications, si l'une des conditions suivantes s'applique :

- Dans un environnement autre que Network Deployment, vous avez ajouté manuellement la configuration du collecteur de données pour l'instance de serveur d'applications et souhaitez annuler la configuration de la collecte de données. L'instance de serveur d'applications doit être en cours d'exécution.
- Dans un environnement Network Deployment, vous avez ajouté manuellement la configuration du collecteur de données pour l'instance de serveur d'applications et souhaitez annuler la configuration de la collecte de données. L'agent de noeud et le gestionnaire de déploiement sur le serveur d'applications doivent être en cours d'exécution.
- Dans un environnement Network Deployment, vous avez configuré l'instance de serveur d'applications pour la collecte des données manuellement et le serveur d'applications ne démarre pas. L'agent de noeud et le gestionnaire de déploiement sur le serveur d'applications doivent être en cours d'exécution.

Si vous avez configuré une instance de serveur d'applications autonome pour la collecte des données manuellement ou avec l'utilitaire de configuration ou de migration et que le serveur d'applications ne démarre pas, vous devez restaurer la configuration WebSphere Application Server avec la configuration sauvegardée. Pour plus d'informations, voir «Restauration de la configuration du serveur d'applications depuis une sauvegarde», à la page 812.

A faire :

- Vous devez apporter des modifications manuelles à la configuration WebSphere Application Server pour les collecteurs de données en tant qu'administrateur WebSphere.
- Les modifications manuelles dans WebSphere Application Server pour la collecte des données doivent être exécutées par un administrateur WebSphere expérimenté uniquement. Toute erreur dans la modification manuelle de la configuration peut empêcher le démarrage du serveur d'applications.
- Si vous configurez manuellement le collecteur de données pour surveiller des instances de serveur d'application, vous ne pouvez pas employer l'utilitaire d'annulation de configuration pour annuler la configuration du collecteur de données.

Procédure

Pour supprimer manuellement la configuration du collecteur de données, procédez comme suit :

1. Connectez-vous à WebSphere Administration Server Console.
2. Cliquez sur **Serveurs**.
3. Développez **Type de serveur** et sélectionnez **Serveurs d'applications WebSphere**.
4. Cliquez sur le nom du serveur.
5. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java** > **Propriétés supplémentaires : Propriétés personnalisées**.
6. Supprimez les propriétés personnalisées suivantes de la machine JVM, si elles existent :
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain. primaryInjectorFile`
7. Identifiez les arguments de JVM qui ont été ajoutés pour le collecteur de données.
   a. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
   b. Si vous avez configuré le serveur d'applications pour la collecte de données manuellement, localisez les arguments JVM que vous avez ajoutés manuellement. Si vous avez configuré le serveur d'applications pour la collecte de données à l'aide des utilitaires de configuration, comparez les valeurs des arguments **AM_OLD_ARGS** et **AM_CONFIG_JVM_ARGS** pour déterminer quels arguments ont été ajoutés par l'utilitaire de configuration.
8. Cliquez sur **Serveur** > **Serveur d'applications** et sélectionnez le nom de serveur approprié.
9. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java**.
10. Dans la zone **Arguments JVM génériques**, retirez les arguments JVM que vous avez identifiés à l'étape 7 pour le collecteur de données.
11. Cliquez sur **Appliquer** ou sur **OK**.
12. Dans la boîte de dialogue **Messages**, cliquez sur **Sauvegarder**.
13. Dans la boîte de dialogue **Sauvegarde dans la configuration maîtresse**, exécutez l'une des étapes suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que la case à cocher **Synchroniser les modifications avec les noeuds** est sélectionnée, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
14. Supprimez les entrées d'environnement qui ont été ajoutés pour le collecteur de données.
    a. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
    b. Selon le système d'exploitation, supprimez l'entrée d'environnement suivante :
       - AIX **LIBPATH**
       - Linux **LD_LIBRARY_PATH**
       - Windows **PATH**
    c. Supprimez l'entrée d'environnement **NLSPATH**.
15. Cliquez sur **Appliquer** ou sur **OK**.
16. Dans la boîte de dialogue **Messages**, cliquez sur **Sauvegarder**.
17. Dans la boîte de dialogue **Sauvegarde dans la configuration maîtresse**, exécutez l'une des étapes suivantes :

- Si vous êtes dans un environnement de déploiement réseau, vérifiez que la case à cocher **Synchroniser les modifications avec les noeuds** est sélectionnée, puis cliquez sur **Sauvegarder**.
- Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.

18. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
19. Supprimez les variables suivantes :
    - **AM_CONFIG_JVM_ARGS**
    - **AM_OLD_JVM_ARGS**
    - **ITCAMDCHOME**
    - **ITCAMDCVERSION**
20. Dans la boîte de dialogue **Messages**, cliquez sur **Sauvegarder**.
21. Dans la boîte de dialogue **Sauvegarde dans la configuration maîtresse**, exécutez l'une des étapes suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que la case à cocher **Synchroniser les modifications avec les noeuds** est sélectionnée, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
22. Si vous avez configuré l'instance de serveur pour la collecte de données à l'aide de l'outil de configuration du collecteur de données, plutôt que manuellement, procédez comme suit :
    a. Accédez au répertoire *base_cd*/runtime.
    b. Renommez le fichier $profile.$cell.$node.$server.input.properties en $profile.$cell.$node.$server.input.properties.bak.
23. Si vous supprimez manuellement la configuration du collecteur de données à partir de toutes les instances de serveur d'applications dans un profil, procédez comme suit :
    a. Accédez au répertoire $appserverhome/bin.
    b. Exécutez la commande **osgiCfgInit.sh/bat -all** sur les systèmes Windows ou la commande **osgiCfgInit.sh -all** sur les systèmes UNIX et Linux.
24. Redémarrez l'instance de serveur d'applications surveillée par le collecteur de données.

Annulation manuelle de la configuration du collecteur de données

Après avoir configuré manuellement le collecteur de données pour l'Agent WebSphere Applications, vous devez annuler la configuration du collecteur de données manuellement pour pouvoir supprimer la collecte de données du serveur d'applications configuré.

Pourquoi et quand exécuter cette tâche

La procédure qui suit s'applique uniquement après avoir configuré manuellement le collecteur de données comme décrit dans «Configuration manuelle du collecteur de données si les utilitaires de configuration échouent», à la page 788. Si vous avez utilisé les utilitaires de configuration pour configurer le collecteur de données, vous devez également utiliser l'utilitaire d'annulation de configuration pour annuler la configuration du collecteur de données. Pour plus d'informations, voir «Annulation de la configuration interactive du collecteur de données», à la page 189 ou «Annulation de la configuration du collecteur de données en mode silencieux», à la page 191.

Procédure

- Pour annuler manuellement la configuration du collecteur de données pour WebSphere Application Server, voir «Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server traditionnel», à la page 196.
- Pour annuler manuellement la configuration du collecteur de données pour le serveur Liberty, voir «Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server Liberty», à la page 196.

Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server traditionnel :
Procédure

1. Connectez-vous à la console d'administration WebSphere en tant qu'administrateur.
2. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Type** et cliquez sur **WebSphere application servers**.
3. Cliquez sur le nom du serveur d'applications.
4. Dans la section **Server Infrastructure** de l'onglet Configuration, développez **Java Virtual Machine** et cliquez sur **Process Definition**.
5. Dans la section **Propriétés supplémentaires**, cliquez sur **Machine virtuelle Java**.
6. Dans la zone **Generic JVM arguments**, supprimez les entrées suivantes du contenu.

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
   toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
   etc/datacollector.policy -verbosegc
   ```

7. Cliquez sur **Appliquer**, puis sur **Sauvegarder**. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
   - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
   - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
8. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Types**, cliquez sur **WebSphere application servers**, puis cliquez sur le nom du serveur.
9. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
10. Selon le système d'exploitation, la plateforme matérielle et la machine virtuelle Java de serveur d'applications utilisés, supprimez l'entrée d'environnement suivante.
    - AIX LIBPATH
    - Linux LD_LIBRARY_PATH
    - Windows PATH
11. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
12. Supprimez la variable *ITCAMDCHOME* si elle existe.
13. Cliquez sur **Appliquer**, puis sur **Sauvegarder**. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
14. Redémarrez l'instance du serveur d'applications.
15. Accédez au répertoire `runtime` dans le répertoire d'installation de l'agent et supprimez le fichier *nom_profil.nom_cellule.nom_noeud.nom_serveur*`.manual.input.properties`.
    - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/runtime/`*profile_name.cell_name.node_name.server_name*`.manual.input.properties`
    - Windows *rép_install*`\dchome\7.3.0.14.06\runtime\`*profile_name.cell_name.node_name.server_name*`.manual.input.properties`

Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server Liberty :

Procédure

1. Accédez au répertoire du serveur Liberty et ouvrez le fichier `jvm.options` dans le répertoire *nom_serveur* au sein du répertoire d'installation du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Supprimez les paramètres suivants du fichier `jvm.options`.

   ```
   -agentlib:am_ibm_16=nom_serveur
   –Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
   -verbosegc
   ```

   où *nom_serveur* est le nom du serveur Liberty et *base_cd* est le répertoire de base du collecteur de données.
3. Ouvrez le fichier `server.xml` et supprimez les lignes suivantes :

   ```
   <feature>webProfile-7.0</feature>
   <feature>monitor-1.0</feature>
   <feature>usr:itcam-730.140</feature>
   ```
4. Ouvrez le fichier `server.env` et supprimez la valeur d'entrée suivante de l'entrée d'environnement selon le système d'exploitation :

Tableau 24. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/aix536`
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/aix536`
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:base_cd/toolkit/lib/lx8266`
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:base_cd/toolkit/lib/li6263`
Windows (machine virtuelle Java 32 bits)	PATH	`/lib;base_cd/toolkit/lib/win32`
Windows (machine virtuelle Java 64 bits)	PATH	`/lib;base_cd/toolkit/lib/win64`

5. Redémarrez le serveur Liberty.
6. Accédez au répertoire `runtime` dans le répertoire d'installation de l'Agent WebSphere Applications et supprimez le fichier *nom_cellule.nom_noeud.nom_serveur*`.manual.input.properties`.
   - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/runtime/`*cell_name.node_name.server_name*`.manual.input.properties`
   - Windows *rép_install*`\dchome\7.3.0.14.06\runtime\`*cell_name.node_name.server_name*`.manual.input.properties`

Agent Node.js : Retrait du plug-in de surveillance

Avant de désinstaller l'Agent Node.js, vous devez retirer le plug-in de surveillance de votre application Node.js.

Procédure

1. Supprimez les plug-in de collecteur de données au début du fichier d'application Node.js :
   - Si vous mettez à niveau l'Agent Node.js à partir de Cloud APM version 8.1.3.2 vers la version 8.1.4, procédez comme suit :
     – Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js :

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
```

où *KNJ_NPM_LIB_LOCATION* correspond au répertoire du dossier `lib` de votre répertoire d'installation global du package npm. Le répertoire par défaut est `/usr/local/lib`.

- Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js :

  ```
  require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
  ```

- Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js :

  ```
  require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
  ```

- Si vous mettez à niveau l'Agent Node.js à partir de Cloud APM version 8.1.3.2 vers la version 8.1.4, procédez comme suit :
  - Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js.

    ```
    require('rép_install/lx8266/nj/bin/plugin/knj_index.js');
    ```

    , où *rép_install* correspond au répertoire d'installation de l'Agent Node.js.
  - Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js.

    ```
    require('rép_install/lx8266/nj/bin/plugin/knj_deepdive.js');
    ```

  - Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js .

    ```
    require('rép_install/lx8266/nj/bin/plugin/knj_methodtrace.js');
    ```

2. Redémarrez l'application Node.js pour désactiver les plug-ins de collecteur de données.
   - Si la version actuelle de votre Agent Node.js estCloud APM version 8.1.3, les plug-ins du collecteur de données sont supprimés dès maintenant.
   - Si la version de votre Agent Node.js actuel est Cloud APM version 8.1.3.2, continuez à l'étape suivante.
3. Exécutez la commande `./uninstall.sh` à partir du répertoire *rép_install*`/lx8266/nj/bin` pour supprimer les paramètres d'agent précédents.

Que faire ensuite

Pour plus d'informations sur la désinstallation de l'Agent Node.js, voir «Désinstallation de vos agents», à la page 187.

agent Microsoft .NET : Retrait du collecteur de données .NET

Avant de désinstaller l'agent Microsoft .NET, vous devez retirer le collecteur de données .NET de vos applications .NET.

Procédure

1. Désenregistrez le collecteur de données. En tant qu'administrateur, entrez :

   ```
   cd rép_install\qe\bin configdc unregisterdc
   ```

   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Arrêtez toutes vos applications .NET pour désactiver le collecteur de données. Entrez `net stop was /y`
3. Pour vous assurer du nettoyage complet du collecteur de données .NET après la désinstallation, suivez ces étapes :

a. Dans l'invite de commande, accédez au répertoire <APM_HOME>\qe\bin.
b. Exécutez le fichier ProcListCaller.bat.
c. Vérifiez le fichier journal CorProfAttach.Log dans le répertoire <APM_HOME>\qe\logs. Le fichier journal répertorie les processus auxquels le composant du profileur du collecteur de données .NET est connecté.
d. Avant de désinstaller l'agent, arrêtez les processus du fichier CorProfAttach.Log.
e. Si aucun processus n'est répertorié, désinstallez l'agent.

Que faire ensuite

Désinstallez l'agent Microsoft .NET. Voir «Désinstallation de vos agents», à la page 187.

Chapitre 10. Configuration de votre environnement

Si votre agent de surveillance requiert une configuration ou que vous souhaitez consulter les paramètres par défaut d'un agent, suivez les étapes fournies pour votre agent.

Connectivité réseau

Dans certaines situations, la connectivité au serveur Performance Management doit être configurée manuellement. Si vous voulez utiliser le protocole HTTPS, ou si vos règles de pare-feu bloquent certaines connexions, vous devez configurer votre système.

Si vous utilisez le protocole HTTPS pour vos communications sécurisées, vous devez activer TLS 1.2 et les chiffrements. Pour plus d'informations, voir Communication sécurisée.

Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer vos agents de sorte qu'ils envoient le trafic à un proxy direct. Pour plus d'informations, voir Configuration des agents pour qu'ils communiquent via un proxy direct.

Communication sécurisée

Le protocole HTTP est utilisé par défaut pour la communication entre les agents et le serveur Cloud APM.

Si vous choisissez d'utiliser le protocole HTTPS pour la communication de l'agent serveur, TLS 1.2 et les suites de chiffrement FIPS Suite B doivent être activés. Les chiffrements suivants sont utilisés :

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

Si vous utilisez HTTPS, les communications du navigateur au serveur nécessitent TLS 1.2. TLS 1.2 n'est pas activé par défaut sur certains navigateurs ; il doit alors être activé manuellement.

Configuration des agents pour qu'ils communiquent via un proxy direct

Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous devez configurer les agents de surveillance IBM de sorte qu'ils envoient le trafic à un proxy direct. Editez la variable d'environnement `KDH_FORWARDPROXY` pour configurer les agents de sorte qu'ils communiquent via un proxy direct.

Pourquoi et quand exécuter cette tâche

Lorsqu'un proxy direct est utilisé, l'agent ouvre au préalable une connexion TCP au proxy. L'agent envoie une demande HTTP CONNECT et l'URL du noeud final cible (serveur Cloud APM) au proxy direct. Le proxy direct établit alors une connexion TCP au noeud final cible et crée une session de tunnellisation HTTP ou HTTPS entre l'agent et le serveur Cloud APM.

© Copyright IBM Corp. 2015, 2018

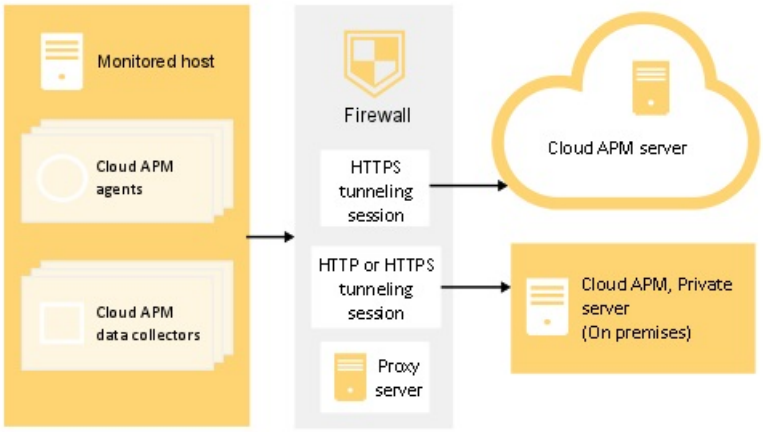


Figure 1. Diagramme de connexion pour l'utilisation d'un proxy direct

L'agent de surveillance ne prend pas en charge les proxys d'authentification, ce qui signifie que l'agent ne prend pas en charge la connexion à un proxy direct à l'aide d'un ID utilisateur et d'un mot de passe de proxy configurés.

Procédure

1. Ouvrez le fichier de configuration d'environnement d'agent dans un éditeur de texte :

   Linux AIX Fichier *rép_install*`/config/global.environment`, où *rép_install* est le répertoire de base d'installation des agents. Le fichier `global.environment` configure tous les agents dans le répertoire d'installation.

   Les paramètres personnalisés du fichier `.global.environment` sont perdus après la mise à niveau de l'agent. Pour conserver vos paramètres, effectuez les modifications de personnalisation dans les fichiers `global.environment`. Les paramètres de ce fichier ne sont pas écrasés par une mise à niveau de l'agent.

   Windows Fichier *rép_install*`\TMAITM6_x64\K`*cp*`ENV` pour les agents 64 bits et fichier *rép_install*`\TMAITM6\K`*cp*`ENV` pour les agents 32 bits où *cp* est le code produit de l'agent. Configurez le fichier `K`*cp*`ENV` pour chaque agent.

   Pour une liste des codes produit, voir «Utilisation des commandes de l'agent», à la page 213.
2. Editez la variable d'environnement `KDH_FORWARDPROXY` pour indiquer l'adresse et le port du proxy :

   `KDH_FORWARDPROXY=`*`http://adresse-proxy:numéro-port-proxy`*

   Par exemple :

   `KDH_FORWARDPROXY=http://HostA:8085`
3. Redémarrez l'agent pour implémenter les modifications. Voir «Utilisation des commandes de l'agent», à la page 213.

Configuration des collecteurs de données pour qu'ils communiquent via un proxy direct

Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer les collecteurs de données pour l'envoi du trafic à un proxy direct. Editez la variable d'environnement `APM_GW_PROXY_CONNECTION` pour configurer les collecteurs de données pour la communication via un proxy direct.

Pourquoi et quand exécuter cette tâche

Lorsqu'un proxy direct est utilisé, le collecteur de données ouvre au préalable une connexion TCP au proxy. Le collecteur de données envoie une demande de connexion et l'URL du noeud final cible (serveur Cloud APM, Private) au proxy direct. Le proxy direct établit alors une connexion TCP au noeud final cible et crée une session de tunnellisation HTTP ou HTTPS entre le collecteur de données et le serveur Cloud APM, Private.

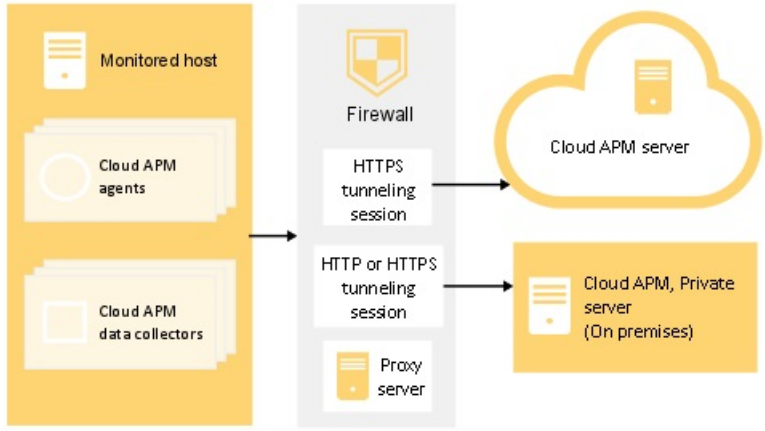


Figure 2. Diagramme de connexion pour l'utilisation d'un proxy direct

Certains collecteurs de données prennent en charge des proxy d'authentification, comme par exemple les collecteurs de données Node.js et Liberty. Ils prennent en charge la connexion à un proxy direct en utilisant un ID utilisateur et un mot de passe de proxy configuré.

Procédure

1. Pour configurer la communication de proxy direct pour les collecteurs de données Python, exécutez l'une des étapes suivantes :
   - Ouvrez le fichier de propriétés `<base_cd>/config.properties` du collecteur de données dans un fichier d'éditeur de texte, <*base_cd*> représentant le répertoire de base d'installation des collecteurs de données, par exemple, `/usr/lib/python2.7/site-packages/ibm_python_dc`. Mettez à jour la variable `APM_GW_PROXY_CONNECTION` avec l'hôte et le numéro de port du proxy, par exemple `APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085`. La modification de la variable dans ce fichier a une incidence sur toutes les applications dans lesquelles le collecteur de données Python est activé.

     Remarque : Pour configurer la communication d'un proxy direct pour une seule application, copiez le fichier `<base_cd>/config.properties` dans le répertoire de l'application unique. Mettez à jour la variable `APM_GW_PROXY_CONNECTION` dans le répertoire de l'application.
   - Exécutez la commande suivante sur des systèmes Linux :

     ```
     export APM_GW_PROXY_CONNECTION =http://<hôte du proxy http>:<port du proxy http>
     ```

     par exemple,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
2. Pour configurer la communication de proxy direct pour les collecteurs de données Node.js, exécutez l'une des étapes suivantes :
   - Exécutez la commande suivante sur des systèmes Linux :

     ```
     export APM_GW_PROXY_CONNECTION =http://<hôte du proxy http>:<port du proxy http>
     ```

     par exemple,

```
export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
```

- Si un nom d'utilisateur et un mot de passe sont requis pour l'accès au serveur proxy direct pour les collecteurs de données Node.js, exécutez la commande suivante sur des systèmes Linux :

  ```
  export APM_GW_PROXY_CONNECTION =http://<utilisateur proxy http>:
  <mot de passe proxy http>@<hôte proxy http>:<port proxy http>
  ```

  par exemple,

  ```
  export APM_GW_PROXY_CONNECTION =http://Joe:passw0rd@9.181.138.247:8085
  ```

3. Pour configurer la communication du proxy direct pour les collecteurs de données Liberty, modifiez le fichier *<base serveur Liberty>*/jvm.options, où *<base serveur Liberty>* est le répertoire de base du serveur Liberty, par exemple : /opt/ibm/wlp/usr/servers/defaultServer/jvm.options. Effectuez l'une des étapes suivantes :
   - Si l'authentification n'est pas requise, ajoutez le code suivant au fichier jvm.options :

     ```
     -Dhttp.proxyHost=<hôte proxy http>
     -Dhttp.proxyPort=<port proxy http>
     -Dhttps.proxyHost=<hôte proxy https>
     -Dhttps.proxyPort=<port proxy https>
     -Djava.net.useSystemProxies=true
     ```

   - Si un nom d'utilisateur et un mot de passe sont requis pour accéder au serveur proxy direct, ajoutez le code suivant au fichier jvm.options :

     ```
     -Dhttp.proxyHost=<hôte proxy http>
     -Dhttp.proxyPort=<port proxy http>
     -Dhttp.proxyUser=<utilisateur proxy http>
     -Dhttp.proxyPassword=<mot de passe proxy http>
     -Dhttps.proxyHost=<hôte proxy https>
     -Dhttps.proxyPort=<port proxy https>
     -Dhttps.proxyUser=<utilisateur proxy https>
     -Dhttps.proxyPassword=<mot de passe proxy https>
     -Djava.net.useSystemProxies=true
     ```

4. Redémarrez l'application locale pour implémenter les modifications.

Résultats

Vous avez configuré vos collecteurs de données pour qu'ils communiquent via un proxy direct.

Noms de systèmes gérés

Le nom de système géré (MSN) est utilisé pour identifier chaque agent Cloud APM dans votre environnement. Il s'agit également du nom d'instance qui apparaît sur le Tableau de bord d'Application Performance lorsque vous sélectionnez un groupe pour chaque système géré à partir de la section **Groupes** du navigateur. Pour éviter tout conflit, affectez des MSN uniques à vos agents.

Le format du MSN de l'agent varie en fonction du type d'agent. Il peut appartenir à l'une des catégories suivantes :

- «Format de MSN commun pour les agents à instance unique»
- «Format de MSN commun pour les agents multi-instance», à la page 205
- «Format de MSN spécial», à la page 206

Format de MSN commun pour les agents à instance unique

Pour la plupart des agents à instance unique, le format commun du MSN est le suivant :

nom_hôte:*pc*

où :

- *nom_hôte* est le nom de l'ordinateur sur lequel l'agent est installé. Cette partie peut être modifiée au besoin.
- *pc* est le code d'agent à deux caractères en majuscules qui est non modifiable. Pour plus d'informations sur les codes des agents, voir «Utilisation des commandes de l'agent», à la page 213.
- **:** est le séparateur qui est non modifiable.

Exemple : `linuxhost01:LZ` est le MSN de l'Agent Linux OS.

Les agents à instance unique qui ne respectent pas ce format de MSN sont répertoriés dans le tableau 25, à la page 206.

Le MSN est limité à 32 caractères. Pour cette catégorie de MSN, 29 caractères peuvent être saisis pour le nom d'hôte car le code agent et le séparateur ne peuvent pas être modifiés.

Important : Si la longueur du MSN dépasse 32 caractères, une partie du MSN est tronquée et le MSN ne s'affiche pas correctement dans la console Cloud APM. Par exemple, si votre nom d'hôte est `VeryLongSalesDivisionServerName03`, votre nom de système géré doit être `VeryLongSalesDivisionServerName03:PC`, mais il sera tronqué à `VeryLongSalesDivisionServerName0`.

Format de MSN commun pour les agents multi-instance

Pour la plupart des agents multi-instance, le format commun du MSN est le suivant :
nom_instance:*nom_hôte*:*pc*

où :

- *nom_instance* est le nom de l'instance d'agent que vous spécifiez lors de la configuration de l'agent. Utilisez cette variable afin de garantir un MSN unique pour chaque instance de type d'agent sur chaque ordinateur hôte d'agent.

  A faire :
  - Les lettres de l'alphabet latin (a-z, A-Z), les chiffres arabes (0-9) et le trait d'union (-) peuvent être utilisés pour créer les noms d'instance d'agent.
  - Le caractère de soulignement (_) n'est pas autorisé dans les noms d'instance d'agent.
  - Le nom d'instance que vous indiquez est limité de la façon suivante :
    - Linux AIX 28 caractères moins la longueur de votre nom d'hôte sur les systèmes Linux ou AIX.
    - Windows 28 caractères moins la longueur de votre nom d'hôte lorsqu'un fichier de réponses silencieux est utilisé pour la configuration sur les systèmes Windows. Par exemple, si `Server-Name` comporte 11 caractères, les instances d'agent sur l'hôte `Server-Name` doivent donc comporter au maximum 17 caractères.
    - Windows 20 caractères moins la longueur par laquelle votre nom d'hôte dépasse 8 caractères lorsque la configuration de la console Cloud APM est utilisée sur les systèmes Windows. Par exemple, si `TestServer` comporte 10 caractères, qui dépasse 8 fois 2, les instances d'agent sur l'hôte `TestServer` doivent donc comporter au maximum 18 caractères.
- *nom_hôte* est le nom de l'ordinateur sur lequel l'agent est installé. Le composant de nom d'hôte du MSN peut être modifié si nécessaire.
- *pc* est le code d'agent à deux caractères en majuscules qui est non modifiable. Pour plus d'informations sur les codes des agents, voir «Utilisation des commandes de l'agent», à la page 213.
- **:** est le séparateur et ne peut pas être modifié.

Exemple : `jboss1:win2016:JE` est le MSN de l'agent JBoss.

Les agents multi-instance qui ne respectent pas ce format de MSN sont répertoriés dans le tableau 25.

Le MSN est limité à 32 caractères. Pour cette catégorie de MSN, 28 caractères peuvent être saisis entre le nom d'instance et le nom d'hôte car le code agent et le séparateur ne peuvent pas être modifiés.

Important : Si la longueur du MSN dépasse 32 caractères, une partie du MSN est tronquée et le MSN ne s'affiche pas correctement dans la console Cloud APM. Par exemple, si vous indiquez `VeryLongInstanceName` comme nom d'instance et que le nom de serveur est `Production09`, le nom du système géré doit être `VeryLongInstanceName:Production09:`*`PC`*. Toutefois, il sera tronqué à `VeryLongInstanceName:Production0`.

Format de MSN spécial

Le format de MSN spécial s'applique aux agents dont les MSN ne respectent pas les deux formats communs de MSN décrits ci-dessus. Ces agents sont répertoriés dans le tableau 25.

Le MSN spécial est limité à 32 caractères. Dans le tableau 25, seules les chaînes en italique figurant la colonne du format de MSN peuvent être modifiées.

Tableau 25. Format de MSN spécial

Agents	Format de MSN	Exemple de MSN
agent Amazon EC2	`B5:`*`nom_sousnoeud_ec2`*`:INS`	`B5:sales:INS`
agent Amazon ELB	• `AL:`*`nom_instance`*`A:APP` • `AL:`*`nom_instance`*`C:CLA` • `AL:`*`nom_instance`*`N:NET`	• `AL:elb-inst3A:APP` • `AL:elb-inst3C:CLA` • `AL:elb-inst3N:NET`
Agent Azure Compute	`AK:`*`nom_sousnoeud_azure_compute`*`:AVM`	`AK:azc-inst3:AVM`
agent Citrix VDI	`VD:`*`nom_site_citrix`*`:XDS`	`VD:xds1:XDS`
agent DataPower	`BN:`*`nom_système_datapower`*`:DPS`	`BN:datapower23:DPS`
agent HTTP Server	`HU:`*`alias_nomhôte`*`:HUS`	`HU:docker-ihs_httpd:HUS`
agent IBM Integration Bus	*`nom_courtier_surveillé`*`:`*`IDagent`*`:KQIB`	`TRADEBRK:AGT1:KQIB`
Agent MQ Appliance	`MK:`*`nomsection_nomhôte`*`:ARM`	`MK:bvtmin_linux150:ARM`
Agent Node.js	`NJ:`*`port_nomhôte`*`:NJA`	`NJ:KVM-014179_3000:NJA`
Agent Oracle Database	• `RZ:`*`nomhôte-nominstance_connexionbdd`*`:ASM` • `RZ:`*`nomhôte-nominstance_connexionbdd`*`:DG` • `RZ:`*`nomhôte-nominstance_connexionbdd`*`:RDB`	`RZ:11g-oracledbdemo-GVT-1BL:RDB`
Agent Ruby	`KM:`*`nomapp_nomhôte`*`:RAP`	`KM:nc9098036112_Blog:RAP`
Agent SAP	• Instance SAP : *`numéroinstance_IDs_nominstance-nomhôte`*`:Ins` • SAP Process Integration : *`nominstance-nomhôte`*`:PI` • SAP Solution Manager : *`nominstance-nomhôte`*`:Slm` • Système SAP : *`nominstance-nomhôte`*`:Sys`	• `PS5-IBMSAP3V1_PS5_11:Ins` • `PS5-IBMSAP3V1:PI` • `PS8-IBMSAP3V3:Slm` • `PS5-IBMSAP3V1:Sys`

Tableau 25. Format de MSN spécial (suite)

Agents	Format de MSN	Exemple de MSN
Agent SAP HANA Database	• Base de données SAP Hana : S7:*nombdd-IDsystèmes*:HDB • Système SAP Hana : *nominstance*:*nomhôte*:S7	• S7:HNA-HNA:HDB • HNA:PS8760:S7
Agent SAP NetWeaver Java Stack	• Cluster AS Java de SAP NW : *nominstance*:*nomhôte*:SV • Instance AS Java de SAP NW : SV:*IDsystèmes-IDmvj*:NWJ	• J01:VPT02F17:SV • SV:J01-83309750:NWJ
Agent UNIX OS	*nomhôte*:KUX	worklight17:KUX
Agent WebLogic	WB:*nominstance*:WLS	WB:Server1:WLS
Agent WebSphere Applications	• WebSphere Application Server : *alias_serveur*:*nomhôte*:KYNS • WebSphere Portal Server : *alias_serveur*:*nomhôte*:KYNR • WebSphere Process Server : *alias_serveur*:*nomhôte*:KYNP	simpletrade:worklight17:KYNS
Agent WebSphere MQ	*nom_gest_files_attente_surveillé*:*nomagentMQ*:MQ	TRADEQM:PoC:MQ
agent Windows OS	Primary:*nomhôte*:NT	Primary:TRADEIIS1:NT

Modification du nom de système géré de l'agent

Vous pouvez modifier le nom de système géré des agents Cloud APM de différentes manières. Pour certains agents, la modification du nom de système géré implique de modifier le nom d'hôte et/ou le nom d'instance d'agent dans le nom de système géré. Pour les autres agents, des procédures spécifiques sont requises pour modifier le nom de système géré.

Avant de commencer

Familiarisez-vous avec les formats de nom de système géré et les restrictions de dénomination, comme décrit dans «Noms de systèmes gérés», à la page 204.

Pourquoi et quand exécuter cette tâche

Pour la plupart des agents Cloud APM, vous pouvez utiliser le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte utilisé dans le nom de système géré. Pour modifier le nom d'instance de l'agent dans le nom de système géré pour les agents multi-instance, vous pouvez utiliser le paramètre de configuration de l'agent. Si vous avez configuré l'agent, vous devez le reconfigurer pour lui attribuer un autre nom d'instance. Une fois que vous avez reconfiguré l'agent, vous ne pourrez pas récupérer les données collectées par l'instance d'agent précédente.

Selon la partie du nom de système géré que vous voulez modifier, vous ne pourrez peut-être pas modifier le nom de système géré en utilisant une seule procédure.

Pour obtenir la méthode de modification du nom de système géré pour l'agent de votre choix, voir le tableau 26, à la page 208.

Exception : La modification du nom de système géré n'est pas prise en charge par l'agent HTTP Server, l'Agent Node.js ou l'Agent Synthetic Playback.

Tableau 26. Méthodes de modification du nom de système géré pour les agents Cloud APM

Déploiement d'agents	Méthode de modification du nom de système géré
agent Amazon EC2	Utilisez le paramètre de configuration de l'agent pour modifier le nom du sous-noeud EC2 dans le nom de système géré ; voir «Paramètres de configuration de l'agent Amazon EC2», à la page 244.
agent Amazon ELB	Créez une instance d'agent portant un nouveau nom pour modifier le nom de système géré.
Agent Azure Compute	Utilisez le paramètre de configuration de l'agent pour modifier le nom du sous-noeud dans le nom de système géré ; voir «Paramètres de configuration de l'Agent Azure Compute», à la page 259.
agent Cassandra	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Cisco UCS	Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance de l'agent ; voir «Paramètres de configuration pour l'agent», à la page 268.
agent Citrix VDI	Utilisez le paramètre de configuration de l'agent pour modifier le nom de site Citrix ; voir «Paramètres de configuration de l'agent Citrix VDI», à la page 278.
Agent Db2	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent DataPower	Utilisez le paramètre de configuration de l'agent pour modifier le nom de système géré ; voir «Configuration de l'agent DataPower», à la page 290.
Agent DataStage	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Hadoop	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent HMC Base	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent IBM Integration Bus	«Spécification d'un nom de système géré unique pour agent IBM Integration Bus», à la page 333
agent JBoss	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Linux KVM	Utilisez les paramètres de configuration de l'agent ; voir «Configuration de la surveillance de Linux KVM», à la page 439.

Tableau 26. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)

Déploiement d'agents	Méthode de modification du nom de système géré
Agent Linux OS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft .NET	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft Active Directory	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft Exchange Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft Hyper-V Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft IIS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft Office 365	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
agent Microsoft SQL Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Microsoft SharePoint Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
Agent MongoDB	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent MySQL	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent NetApp Storage	Utilisez les paramètres de configuration de l'agent ; voir «Configuration de la surveillance de NetApp Storage», à la page 542.
Agent OpenStack	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Oracle Database	Utilisez les paramètres de configuration de l'agent ; voir «Configuration de la surveillance d'Oracle Database», à la page 573.

Tableau 26. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)

Déploiement d'agents	Méthode de modification du nom de système géré
Agent PHP	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent PostgreSQL	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent RabbitMQ	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent de surveillance des temps de réponse	«Spécification d'un nom de système géré unique pour l'Agent de surveillance des temps de réponse», à la page 668
Agent Ruby	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.
Agent SAP	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent SAP HANA Database	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent SAP NetWeaver Java Stack	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Siebel	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211. Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 211.

Tableau 26. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)

Déploiement d'agents	Méthode de modification du nom de système géré
Agent Sterling File Gateway	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré». Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Sterling Connect Direct	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré». Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Tomcat	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré». Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent UNIX OS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré».
Agent WebSphere Applications	Pour modifier le nom d'hôte dans le nom de système géré, voir How to change the host name used in managed system name for the WAS agent instance?. Pour modifier le nom de l'alias de serveur dans le nom de système géré, reconfigurez l'agent ; voir «Reconfiguration du collecteur de données en mode interactif», à la page 778.
Agent WebSphere Infrastructure Manager	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré». Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent WebSphere MQ	«Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 860
agent Windows OS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré».

Modification du nom d'hôte dans le nom de système géré

Pourquoi et quand exécuter cette tâche

La modification du nom d'hôte dans le nom de système géré n'est pas une pratique courante. En effet, le nom d'hôte est automatiquement détecté et défini lors de la configuration de l'agent. Ne modifiez le nom d'hôte dans le nom de système géré que si nécessaire et vérifiez que la valeur que vous spécifiez n'insère pas de troncatures en raison des restrictions de dénomination du nom de système géré.

Procédure

1. Arrêtez toutes les instances existantes de l'agent et attendez que la console Cloud APM indique que l'agent ou ses sous-noeuds soient hors ligne. S'il n'en existe aucune, passez à l'étape suivante.

Pour plus d'informations sur l'arrêt des instances d'agent, voir «Utilisation des commandes de l'agent» , à la page 213.

2. Si l'agent est un agent à instance unique, procédez comme suit pour modifier le paramètre **CTIRA_HOSTNAME**. La valeur que vous spécifiez pour le paramètre **CTIRA_HOSTNAME** est celle qui est appliquée à toutes les nouvelles instances d'agent.
   a. Effectuez une copie de sauvegarde du fichier suivant :
      - Linux AIX *rép_install*/config/*cp*.environment
      - Windows *rép_install*\TMAITM6_x64\k*pc*cma.ini

      où :
      - *rép_install* est le répertoire d'installation de l'agent.
      - *pc* est le code d'agent à deux caractères. Voir le tableau Noms et codes d'agent.
   b. Editez le fichier en modifiant la valeur de paramètre **CTIRA_HOSTNAME** comme suit, où *nouveau_nom_hôte* est la chaîne personnalisée utilisée à la place du nom d'hôte réel de l'ordinateur sur lequel l'agent est installé.
      - Linux AIX **CTIRA_HOSTNAME**=*nouveau_nom_hôte*
      - Windows **CTIRA_HOSTNAME**=*nouveau_nom_hôte* .TYPE=REG_EXPAND_SZ
   c. Sauvegardez vos modifications.
3. Si l'agent est un agent multi-instance, procédez comme suit pour modifier le paramètre **CTIRA_HOSTNAME**. En général, toutes les instances d'agent sur un ordinateur utilisent la même valeur de nom d'hôte. Si vous souhaitez en utiliser une autre, modifiez la valeur que vous avez indiquée dans **CTIRA_HOSTNAME** lors de l'exécution de cette étape.
   a. Effectuez une copie de sauvegarde des fichiers suivants :
      - Linux AIX *rép_install*/config/*pc_instance*.environment
      - Windows *rép_install*\TMAITM6_x64\k*pc*cma_*instance*.ini
   b. Editez le fichier en modifiant la valeur du paramètre **CTIRA_HOSTNAME** comme suit :
      - Linux AIX **CTIRA_HOSTNAME**=*nouveau_nom_hôte*
      - Windows **CTIRA_HOSTNAME**=*nouveau_nom_hôte* .TYPE=REG_EXPAND_SZ
   c. Sauvegardez vos modifications.
4. Windows Reconfigurez les instances d'agent existantes.
5. Démarrez toutes les instances de l'agent.

Que faire ensuite

Une fois que vous avez modifié le nom de système géré de l'agent, démarrez la console Cloud APM et modifiez vos applications en remplaçant l'ancien nom de système géré des applications par le nouveau.

Configuration d'agents

Après l'installation, certains agents sont configurés et démarrés automatiquement, alors que d'autres nécessitent une configuration manuelle mais démarrent automatiquement. Certains agents doivent être configurés et démarrés manuellement. Les agents multi-instances nécessitent la création d'une première instance et un démarrage manuel.

Avant de commencer

Lorsque vous installez un agent, un exemple de fichier de configuration silencieux est placé dans le répertoire `/opt/ibm/apm/agent/samples`, par exemple, `ynv_silent_config_agent.txt` et `datapower_silent_config.txt`.

Remarque : Certains agents, tels que l'Monitoring Agent for WebSphere Applications, ont plusieurs fichiers de configuration en mode silencieux pour différentes tâches telles que la configuration du collecteur de données.

Pourquoi et quand exécuter cette tâche

Pour obtenir des détails sur le déploiement des agents, voir Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155.

Pour configurer un agent, vous pouvez utiliser la ligne de commande ou un fichier de réponses silencieux tel que décrit dans cette procédure.

Les méthodes de configuration varient en fonction des agents. Suivez la procédure fournie pour votre agent.

Procédure

- Exécutez la commande *nom-agent*`.sh config`. Pour plus de commandes, voir le tableau 28, à la page 215 et le tableau 29, à la page 216.
- Editez le fichier de réponses silencieux, puis exécutez l'une des commandes suivantes :
  - Pour les agents à instance unique, exécutez la commande suivante :
    nom-agent`.sh config` *fichier_réponses*
  - Pour les agents à plusieurs instances, exécutez la commande suivante :
    nom-agent`.sh config` *nom_instance fichier_réponses*
  - où *nom_instance* est le nom de l'instance qui peut être attribué pour indiquer ce que vous surveillez.
- Windows Pour les agents pris en charge sur les systèmes Windows, vous pouvez effectuer certaines tâches de configuration à l'aide de la fenêtre IBM Cloud Application Performance Management. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**. Pour plus d'informations, voir «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 217.
- Pour effectuer une configuration avancée pour certains agents, comme la configuration du suivi des transactions ou de la collecte des données, et l'activation des données de diagnostic, utilisez la fenêtre Configuration d'agent. Pour plus d'informations, voir «Page Configuration d'agent», à la page 218.

Utilisation des commandes de l'agent

Les scripts qui sont utilisés pour installer les agents de surveillance sont également utilisés pour vérifier le statut d'un agent installé, l'arrêter, le démarrer ou le désinstaller.

Pourquoi et quand exécuter cette tâche

Le nom d'agent et les codes agent sont fournis à titre de référence.

Utilisez le nom de l'agent dans les commandes suivantes :

Linux AIX *nom*`-agent.sh`

Windows *nom*`-agent.bat`

où *nom* correspond au nom de l'agent qui est spécifié dans le tableau 27.

Tableau 27. Noms et codes d'agent

Agent de surveillance	*nom*	**Code agent à deux lettres**
Monitoring Agent for Amazon EC2	`amazon_ec2`	`b5`
Monitoring Agent for Azure Compute	`azure_compute`	`ak`

Tableau 27. Noms et codes d'agent (suite)

Agent de surveillance	*nom*	**Code agent à deux lettres**
Monitoring Agent for Cassandra	cassandra	zc
Monitoring Agent for Cisco UCS	cisco_ucs	v6
Monitoring Agent for Citrix Virtual Desktop Infrastructure	citrix_vdi	vd
Monitoring Agent for DataPower	datapower	bn
Monitoring Agent for Db2	db2	ud
Monitoring Agent for Hadoop	hadoop	h8
Monitoring Agent for HMC Base	hmc_base	ph
Monitoring Agent for HTTP Server	http_server	hu
Monitoring Agent for IBM Integration Bus	iib	qi
Monitoring Agent for MQ Appliance	ibm_mq_appliances	mk
Monitoring Agent for InfoSphere DataStage	datastage	dt
Monitoring Agent for JBoss	jboss	je
Monitoring Agent for Linux KVM	linux_kvm	v1
Monitoring Agent for Linux OS	os	lz
Monitoring Agent for Microsoft Active Directory	msad	3z
Monitoring Agent for Microsoft Cluster Server	mscs	q5
Monitoring Agent for Microsoft Exchange Server	msexch	ex
Monitoring Agent for Microsoft Hyper-V Server	microsoft_hyper-v_server	hv
Monitoring Agent for Microsoft Internet Information Services	msiis	q7
Monitoring Agent for Skype for Business Server (anciennement Microsoft Lync Server)	skype_for_business_server	ql
Monitoring Agent for Microsoft .NET	dotnet	qe
Monitoring Agent for Microsoft Office 365	microsoft_office365	mo
Monitoring Agent for Microsoft SharePoint Server	ms_sharepoint_server	qp
Monitoring Agent for Microsoft SQL Server	mssql	oq
Monitoring Agent for MongoDB	mongodb	kj
Monitoring Agent for MySQL	mysql	se
Monitoring Agent for NetApp Storage	netapp_storage	nu
Monitoring Agent for Node.js	nodejs	nj
Monitoring Agent for OpenStack	openstack	sg
Monitoring Agent for Oracle Database	oracle_database	rz
Monitoring Agent for PHP	php	pj
Monitoring Agent for PostgreSQL	postgresql	pn
Monitoring Agent for Python	python	pg
Monitoring Agent for RabbitMQ	rabbitMQ	zr
Monitoring Agent for Ruby	ruby	km
Monitoring Agent for SAP Applications	sap	sa
Monitoring Agent for SAP HANA Database	sap_hana_database	s7

Tableau 27. Noms et codes d'agent (suite)

Agent de surveillance	*nom*	**Code agent à deux lettres**
Monitoring Agent for SAP NetWeaver Java Stack	`sap_netweaver_java_stack`	`sv`
Monitoring Agent for Siebel	`siebel`	`uy`
Monitoring Agent for Sterling Connect Direct	`sterling_connect_direct-agent`	`FC`
Monitoring Agent for Sterling File Gateway	file_gateway	fg
Monitoring Agent for Sybase Server	sybase	oy
Monitoring Agent for Synthetic Playback	`synthetic_transactions`	`sn`
Monitoring Agent for Tomcat	`tomcat`	`ot`
Monitoring Agent for UNIX OS	`os`	`ux`
Monitoring Agent for VMware VI	`vmware_vi`	`vm`
Monitoring Agent for WebLogic	`oracle_weblogic`	`wb`
Monitoring Agent for WebSphere Applications	`was`	`yn`
Monitoring Agent for WebSphere Infrastructure Manager	`wim`	`d0`
Monitoring Agent for WebSphere MQ	`mq`	`mq`
Monitoring Agent for Windows OS	`os`	`nt`
Agent de surveillance des temps de réponse	`rt`	`t5`

Procédure

- Linux AIX Sur le système ou la machine virtuelle où vous voulez envoyer une commande à l'agent de surveillance, accédez au répertoire *rép_install*`/bin`. Entrez n'importe laquelle des commandes du tableau 28 où *nom* correspond au nom de l'agent spécifié dans le tableau 27, à la page 213.

Tableau 28. Commandes pour les systèmes AIX et Linux

Commande	**Description**
`./`*nom*`-agent.sh status`	Vérifie le statut de l'agent. Le statut peut être "en cours d'exécution" ou "pas en cours d'exécution". Lorsque l'agent est en cours d'exécution, le statut de la connexion entre l'agent et le serveur Cloud APM est également vérifié. Les statuts de connexion négative possibles sont : Connection failed, Error detected, Disconnected-error. Le statut de connexion positive est Connected ; il s'agit du statut attendu. Le statut transitionnel est Connecting. Le statut Unknown indique que le statut de l'agent ne peut pas être reconnu, probablement en raison d'erreurs dans le système de fichiers ou dans le fichier journal de l'agent.
`./`*nom*`-agent.sh start`	Démarre l'agent de surveillance. Si l'agent possède des instances, entrez un nom d'instance après la commande.
`./`*nom*`-agent.sh stop`	Arrête l'agent. Si l'agent possède des instances, entrez un nom d'instance après la commande.
`./`*nom*`-agent.sh prereqcheck`	Exécute une analyse prérequise. Cette option de commande est disponible pour la plupart des agents.

Tableau 28. Commandes pour les systèmes AIX et Linux (suite)

Commande	Description
`./nom-agent.sh install`	Installe l'agent de surveillance. Pour plus d'informations, voir «Installation des agents sur les systèmes AIX», à la page 165 et «Installation des agents sur les systèmes Linux», à la page 170.
`./nom-agent.sh config nom_instance chemin_fichier_config_silencieux`	Configure l'agent de surveillance. Exécutez la commande à partir du répertoire *rép_install*`/bin` et ajoutez si nécessaire le chemin du fichier de réponses. Si l'agent possède plusieurs instances, entrez un nom d'instance. Pour plus d'informations sur les agents qui possèdent plusieurs instances, voir tableau 23, à la page 156 . *fichier_config_silencieux* est facultatif. Si vous ne spécifiez pas un fichier pour la configuration en mode silencieux, vous pouvez configurer l'agent de surveillance de manière interactive en suivant les invites.
`./name-agent.sh uninstall`	Désinstalle l'agent de surveillance. Pour plus d'informations, voir «Désinstallation de vos agents», à la page 187.
`./smai-agent.sh uninstall_all`	Désinstalle tous les agents de surveillance sur le système géré.
`./nom-agent.sh remove nom_instance`	Supprime une instance d'un agent à plusieurs instances.
`./nom-agent.sh`	Affiche une description des fonctions disponibles avec le script.

- Windows Sur le système ou la machine virtuelle où vous voulez envoyer une commande à l'agent de surveillance, accédez au répertoire *rép_install*`\BIN` à l'invite de commande, par exemple : `C:\IBM\APM\bin`. Entrez n'importe laquelle des commandes du tableau 29 où *nom* correspond au nom de l'agent spécifié dans le tableau 27, à la page 213.

Tableau 29. Commandes pour les systèmes Windows

Commande	Description
nom`-agent.bat status`	Vérifie le statut de l'agent. Vérifie le statut de la connexion entre l'agent et le serveur Cloud APM. Les statuts de connexion négative possibles sont : Connection failed, Error detected, Disconnected-error. Le statut de connexion positive est Connected ; il s'agit du statut attendu. Le statut transitionnel est Connecting. Le statut Unknown indique que le statut de l'agent ne peut pas être reconnu, probablement en raison d'erreurs dans le système de fichiers ou dans le fichier journal de l'agent.
nom`-agent.bat start`	Démarre l'agent de surveillance. Si l'agent possède des instances, entrez un nom d'instance après la commande.
nom`-agent.bat stop`	Arrête l'agent. Si l'agent possède des instances, entrez un nom d'instance après la commande.
nom`-agent.bat prereqcheck`	Exécute une analyse prérequise. Cette option de commande est disponible pour la plupart des agents.
nom`-agent.bat install`	Installe l'agent de surveillance. Pour plus d'informations, voir «Installation d'agents», à la page 180.

Tableau 29. Commandes pour les systèmes Windows (suite)

Commande	Description
nom-agent.bat config *nom_instance chemin_fichier_config_silencieux*	Configure l'agent de surveillance. Exécutez la commande à partir du répertoire *rép_install*\bin et ajoutez si nécessaire le chemin du fichier de réponses. Si l'agent possède plusieurs instances, entrez un nom d'instance. Pour plus d'informations sur les agents qui possèdent plusieurs instances, voir tableau 23, à la page 156 . *fichier_config_silencieux* est facultatif. Si vous ne spécifiez pas un fichier pour la configuration en mode silencieux, vous pouvez configurer l'agent de surveillance de manière interactive en suivant les invites.
nom-agent.bat uninstall	Désinstalle l'agent de surveillance. Pour plus d'informations, voir «Désinstallation de vos agents», à la page 187.
smai-agent.bat uninstall_all	Désinstalle tous les agents de surveillance sur le système géré.
nom-agent.bat remove *nom_instance*	Supprime une instance d'un agent à plusieurs instances.
nom-agent.bat	Affiche une description des fonctions disponibles avec le script.

Commande de version d'agent

- Pour afficher la version d'un agent dans votre environnement, exécutez les commandes suivantes :
  - Linux AIX

    rép_install/bin/cinfo

    Entrez 1 pour afficher les versions.
  - Windows

    rép_install\InstallITM\kincinfo

Tâches associées:

«Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows» Les agents pris en charge sous Windows possèdent un utilitaire d'interface graphique que vous pouvez utiliser pour exécuter la configuration de l'agent et vérifier le statut de connexion.

Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows

Les agents pris en charge sous Windows possèdent un utilitaire d'interface graphique que vous pouvez utiliser pour exécuter la configuration de l'agent et vérifier le statut de connexion.

L'utilitaire de configuration d'interface graphique n'est disponible ni pour l'Monitoring Agent for WebSphere MQ, ni pour l'Monitoring Agent for IBM Integration Bus.

Procédure

Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.

Résultats

La fenêtre IBM Cloud Application Performance Management apparaît. Chaque composant d'agent installé est répertorié avec son statut de configuration, qu'il soit démarré ou arrêté, le statut de connexion, le numéro de version et d'autres informations.

Que faire ensuite

Démarrez ou arrêtez un agent ou configurez ses paramètres en cliquant sur l'agent à l'aide du bouton droit de la souris, puis en sélectionnant une option.

Page Configuration d'agent

Utilisez la page Configuration d'agent pour configurer de manière centralisée les paramètres d'agents tels que l'Agent de surveillance des temps de réponse et l'Agent WebSphere Applications.

Utilisation générale

Après avoir cliqué sur **Configuration système** > **Configuration d'agent** dans la barre de navigation, un tableau de bord à onglets s'affiche. Il contient un onglet pour chaque agent de surveillance configurable. Le tableau présente des colonnes comportant des informations de configuration, notamment le nom et l'adresse IP de chaque système géré, avec une ligne pour chaque système géré.

Actions
Utilisez les options Actions pour activer ou désactiver les fonctions telles que le suivi des transactions ou la collecte des données.

Redimensionnement de colonne
Faites glisser la bordure d'un en-tête de colonne pour régler la largeur de la colonne.

Tri de colonne
Cliquez à l'intérieur d'un en-tête de colonne pour procéder au tri en fonction de cette colonne. Cliquez de nouveau sur le même en-tête de colonne pour passer de l'ordre de tri croissant à l'ordre de tri décroissant et inversement.

Filtre de tableau
Cliquez à l'intérieur de la zone de texte de filtre et entrez le début de la valeur qui va servir à filtrer la table. Au fur et à mesure de la saisie, les lignes de table qui ne répondent pas aux critères sont filtrées et la ligne ***Total*** est mise à jour en fonction du nombre de lignes trouvées.

Cliquez sur «x» dans la zone de filtre ou appuyez sur la touche Retour arrière pour désactiver le filtre.

Configuration d'agent

Pour plus d'informations sur les paramètres des agents spécifiques, reportez-vous aux rubriques suivantes :

- agent DataPower: «Configuration de la surveillance DataPower», à la page 281
- agent IBM Integration Bus: «Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 333
- Internet Service Monitoring«Configuration de l'agent sur des systèmes Windows», à la page 415
- agent JBoss: «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 434
- agent Microsoft .NET: «Activation de la collecte des données de suivi des transactions et de diagnostic» , à la page 488

- Surveillance du fichier journal d'agent de système d'exploitation : «Ajout ou suppression de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation», à la page 591
- Agent de surveillance des temps de réponse: «Configuration à l'aide de la page Configuration d'agent», à la page 644
- Géolocalisation : «Personnalisation des valeurs de localisation Transaction utilisateur final», à la page 664
- Agent Ruby: «Désactivation ou activation des données de diagnostic pour les applications Ruby», à la page 676
- Agent SAP NetWeaver Java Stack: «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 705
- Agent Tomcat: «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 741
- Agent WebLogic: «Configuration du suivi des transactions pour l'Agent WebLogic», à la page 758
- Agent WebSphere Applications: «Configuration dynamique de la collecte des données sur la page Configuration d'agent», à la page 808
- Agent WebSphere MQ: «Configuration du suivi des transactions pour l'Agent WebSphere MQ», à la page 862

Configuration des agents en tant qu'utilisateur non superutilisateur

Pour configurer votre agent en tant qu'utilisateur non superutilisateur, créez un groupe commun sur le système et faites de chaque utilisateur un membre de ce groupe.

Avant de commencer

Si vous avez installé votre agent en tant que superutilisateur ou utilisateur non superutilisateur et souhaitez configurer l'agent de la même manière, aucune action spéciale n'est requise.

Si vous avez installé votre agent en tant qu'un utilisateur sélectionné et souhaitez configurer l'agent en tant qu'un autre utilisateur, créez un groupe commun sur le système. Définissez tous les utilisateurs de gestion d'agent comme membres de ce groupe commun. Transférez la propriété de tous les fichiers et répertoires d'agent vers ce groupe.

Remarque :

- Pour l'agent HTTP Server, si vous configurez l'agent en tant qu'utilisateur non superutilisateur, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître le IBM HTTP Server.
- Pour l'agent IBM Integration Bus, si l'installation d'IBM Bus Integration est un déploiement à utilisateur unique, utilisez le même ID utilisateur que l'utilisateur qui a installé IBM Integration Bus pour configurer l'agent. Pour configurer l'agent, procédez comme suit pour cet ID utilisateur.

Procédure

1. Installez vos agents de surveillance sous Linux ou AIX comme décrit dans «Installation des agents sur les systèmes Linux», à la page 170 et «Installation des agents sur les systèmes AIX», à la page 165.
2. Exécutez le script `./secure.sh` avec le nom de groupe de l'utilisateur non superutilisateur afin de sécuriser les fichiers et définissez la propriété de groupe de fichiers sur les fichiers. Par exemple : **`./secure.sh -g db2iadm1`**
3. Configurez vos agents de surveillance sous Linux ou AIX selon vos besoins ; voir Chapitre 10, «Configuration de votre environnement», à la page 201.
4. Pour mettre à jour les scripts de démarrage du système, exécutez le script suivant en tant que superutilisateur ou utilisateur sudo: *rép_install*`/bin/UpdateAutoRun.sh`

Que faire ensuite

Pour plus d'informations sur le script **./secure.sh**, voir Sécurisation des fichiers d'installation de l'agent.

Utilisez le même ID utilisateur pour l'installation et les mises à niveau de l'agent.

Désactivation du démarrage automatique de l'agent sur les systèmes AIX et Linux

Sur le système AIX ou Linux, un agent peut démarrer automatiquement suite au redémarrage du système d'exploitation. Si vous ne voulez pas que l'agent démarre automatiquement après le redémarrage du système, vous pouvez désactiver le démarrage automatique de l'agent.

Pourquoi et quand exécuter cette tâche

Si vous installez un agent en tant que superutilisateur sur le système AIX ou Linux, l'agent peut démarrer automatiquement après avoir redémarré le système. Sinon, si vous installez un agent en tant qu'utilisateur non superutilisateur, mais que vous exécutez le script **UpdateAutoRun.sh** en tant que superutilisateur suite à l'installation, l'agent peut démarrer automatiquement suite au redémarrage du système.

Procédure

Pour désactiver le démarrage automatique de l'agent, procédez comme suit :

1. Ouvrez le fichier *rép_install_agent*/registry/AutoStart.
2. Redéfinissez le contenu sur 0 et sauvegardez vos modifications. Le contenu précédent est un nombre positif, comme 1, 2, 3 ou 4 par exemple, qui spécifie au script d'agent de s'exécuter après le redémarrage du système.

Résultats

Une fois que le système a redémarré, aucun script d'agent ne s'exécute automatiquement pour démarrer l'agent.

Connexion des agents à un autre serveur

Avant d'installer les agents, vous devez configurer le package d'installation afin d'établir la connexion avec le serveur Cloud APM. La configuration du package d'agent s'effectue automatiquement pendant l'installation du serveur, ou manuellement à tout autre moment.

Si vous voulez changer le serveur Cloud APM auquel l'agent se connecte, exécutez le script **agent2server** pour établir la communication avec un autre serveur.

Pourquoi et quand exécuter cette tâche

- Le script **agent2server** est exécuté sur chaque système géré que vous voulez connecter à un autre serveur.
- Le changement de connexion serveur affecte tous les agents installés sur le système géré. Par exemple, si l'Agent Linux OS, l'agent IBM Integration Bus et l'Agent WebSphere MQ sont installés sur le même système, ils sont tous reconnectés au nouveau serveur.
- Le script est exécuté avec une option différente, selon que la communication de l'agent avec le serveur utilise le protocole HTTP ou HTTPS sécurisé.
- Pour les communications HTTPS, une étape supplémentaire est nécessaire pour copier le package de configuration de l'agent du nouveau serveur (cible) vers le système géré. Les informations de serveur dans le package de configuration de l'agent sont utilisées pour modifier le système géré pour la nouvelle adresse du serveur et le certificat de signataire.

Avertissement : Si vous avez l'intention de changer le protocole, HTTP en HTTPS par exemple, suivez les instructions de «Configuration du protocole de communications pour les agents de serveur», à la page 1097 avant d'effectuer la procédure.

Procédure

Pour changer le serveur Cloud APM et connecter l'ensemble des agents installés sur le système géré à un autre serveur, procédez comme suit :

1. Si le système géré utilise les communications HTTPS sécurisées, copiez le package de configuration d'agent du nouveau serveur Cloud APM au système géré. Le package de configuration de l'agent est la sortie du script `make_configuration_packages` qui a été exécuté pour vous lors de l'installation du serveur si vous avez choisi de configurer les images d'agent (voir «Téléchargement et installation du serveur», à la page 141) ou de les exécuter manuellement à un moment ultérieur (voir «Configuration des images téléchargées», à la page 162). Vous copiez le fichier compressé `onprem_config` à partir du répertoire du serveur Cloud APM tel que `/opt/ibm/ccm/agentconfig/`, vers le répertoire de système géré, tel que `/opt/ibm/apm/newagentconfig/onprem_config.tar` ou `\IBM\APM\newagentconfig\onprem_config.zip`.
2. Sur le système géré, accédez au répertoire *rép_install*`/bin`. Exemples :
   - AIX
     ```
     cd /opt/ibm/apm/agent/bin
     ```
   - Linux
     ```
     cd /opt/ibm/apm/agent/bin
     ```
   - Windows
     ```
     cd \IBM\APM\agent\bin
     ```
3. Pour les communications HTTP non sécurisées, exécutez la commande suivante pour configurer les agents de sorte qu'ils se connectent au serveur Cloud APM spécifié. Sinon, passez à l'étape suivante pour les communications HTTPS sécurisées.
   - Linux AIX
     ```
     ./agent2server.sh -s nom_hôte
     ```
   - Windows
     ```
     agent2server.bat -s nom_hôte
     ```

   où *nom_hôte* est l'adresse IP ou le nom de système hôte qualifié complet du système sur lequel le serveur Cloud APM auquel vous voulez vous connecter est installé.
4. Pour les communications HTTPS sécurisées, exécutez la commande permettant de configurer les agents pour le nouveau serveur :
   - Linux AIX
     ```
     ./agent2server.sh -f chemin
     ```
   - Windows
     ```
     agent2server.bat -f chemin
     ```

   où *chemin* est le chemin d'accès au package de configuration d'agent. Cet exemple spécifie le chemin complet vers le package de configuration d'agent sur le système géré Linux : **`agent2server.sh -f`** `/opt/ibm/apm/newagentconfig/onprem_config.tar`. Cet exemple spécifie le chemin relatif au package de configuration d'agent sur le système géré Windows : **`agent2server.bat -f`** `..\..\newagentconfig\onprem_config.zip`

Résultats

Les agents sont reconfigurés pour se connecter au nouveau serveur Cloud APM et les communications sont établies avec le serveur. Si vous avez exécuté le script pour utiliser les communications HTTPS

sécurisées, les agents sont également configurés avec le certificat du signataire pour le nouveau serveur. Les agents ne se connectent plus au serveur initial.

Que faire ensuite

Vous devez configurer les agents du serveur Cloud APM pour utiliser le protocole HTTPS et les certificats ; voir «Configuration du protocole de communications pour les agents de serveur», à la page 1097.

Configuration des certificats entre le serveur et les agents

Pour permettre les communications entre le serveur Cloud APM et les agents, vous pouvez configurer des certificats par défaut, personnalisés ou autosignés.

Configuration d'un certificat par défaut

Si vous utilisez le protocole HTTPS pour communiquer entre le serveur Cloud APM et les agents, le serveur Cloud APM autorise les connexions des ressources qui s'authentifient avec un certificat valide. Vous pouvez configurer les communications HTTPS basées sur les certificats par défaut générés lors de l'installation du serveur Cloud APM.

Avant de commencer

Lors de l'installation du serveur Cloud APM, les certificats du serveur et des agents de l'autorité de certification racine locale signés par cette autorité de certification racine locale sont toujours générés, à moins que le répertoire `/opt/ibm/ccm/keyfiles` n'existe avant le début de l'installation.

- L'autorité de certification racine locale est établie et deux magasins de clés sont générés. Un magasin de clés contient la clé utilisée par le serveur et l'autre, les clés utilisées par les agents.
- Les clés des magasins de clés sont signées par l'autorité de certification racine locale. Les certificats de clé publique sont échangés entre ces magasins de clés. Par exemple, la clé publique signée du serveur est ajoutée au magasin de clés des agents et la clé publique signée des agents est ajoutée au magasin de clés du serveur.
- La clé publique de l'autorité de certification racine locale est ajoutée aux deux magasins de clés pour que l'agent et le serveur puissent faire confiance à leurs certificats.
- Le protocole HTTPS utilise les chiffrements Elliptic Curve sur 256 bits et respecte la norme FIPS Suite-B.

Pourquoi et quand exécuter cette tâche

Les scénarios suivants s'appliquent :

- Si vous avez configuré les agents lors de l'installation du serveur et défini *APM_SECURE_COMMUNICATION=y* , qui active les communications HTTPS, vous n'avez pas besoin d'effectuer d'étapes supplémentaires maintenant pour utiliser le protocole de communication HTTPS.
- Si vous avez configuré les agents lors de l'installation du serveur avec le protocole HTTP par défaut, vous devez maintenant reconfigurer les images d'agent afin de créer de nouveaux modules de configuration pour utiliser le protocole de communication HTTPS. Pour plus d'informations, voir l'étape 1 de la procédure.
- Si vous n'avez pas configuré les agents lors de l'installation du serveur Cloud APM, vous devez configurer les agents avec les communications HTTPS activées entre le serveur et les agents, comme illustré dans la procédure.

Pour activer les communications entre le serveur et les agents à l'aide des certificats par défaut générés lors de l'installation du serveur Cloud APM, effectuez les étapes suivantes :

Procédure

1. Pour configurer les images d'agent manuellement, voir «Configuration des images téléchargées», à la page 162. Assurez-vous de bien sélectionner les communications **HTTPS** lorsque vous exécutez le script `make_configuration_packages.sh` pour créer les modules de configuration.
2. Copiez l'élément xml <ssl> qui contient l'attribut enabledCiphers du fichier *rép_install*`/wlp/usr/servers/min/server.xml` vers le fichier *rép_install*`/wlp/usr/servers/min/user-exit.xml` . Ajoutez ensuite la ligne suivante après la ligne enabledCiphers dans le fichier `user-exit.xml` :

   ```
   clientAuthentication="true"
   ```
3. Pour remplacer le protocole de communication de la configuration centrale d'agent par https, procédez comme suit :
   a. Connectez vous à console Cloud APM.
   b. Sélectionnez **Configuration du système** > **Configuration avancée**.
   c. Cliquez sur **Configuration centrale d'agent**.
   d. Définissez le **Protocole** pour inclure «https», puis cliquez sur **Sauvegarder**.
4. Installez les agents à l'aide des images d'agent configurées à l'étape 1.

Que faire ensuite

Vous devez configurer les agents du serveur Cloud APM pour utiliser le protocole HTTPS et les certificats. Pour obtenir des instructions, voir «Configuration du protocole de communications pour les agents de serveur», à la page 1097.

Configuration d'un certificat autosigné

Vous pouvez décider d'utiliser votre propre certificat au lieu de celui généré par l'autorité de certification ou du certificat par défaut généré par le serveur Cloud APM.

Avant de commencer

Vérifiez que les pare-feux ou les périphériques de filtrage réseau qui se trouvent entre le serveur Cloud APM et les agents de surveillance autorisent les communications sur le port **443**. Vous devez préparer deux mots de passe : un pour le magasin de clés du serveur et l'autre pour celui de l'agent.

Procédure

Si vous souhaitez utiliser un certificat signé par vos soins, procédez comme suit :

1. Connectez-vous au système d'exploitation de la machine du serveur et au répertoire `KEYFILES_DIR` qui correspond au répertoire `/opt/ibm/ccm/keyfiles`.
2. Pour générer une autorité de certification racine locale afin de signer les demandes de signature de certificat du serveur et les certificats des agents, vous devez choisir un mot de passe. Ce mot de passe chiffre la clé privée de l'autorité de certification racine et le magasin de clés. Vous devez ensuite définir le mot de passe comme variable d'environnement. L'outil de sécurité utilisé pour la gestion des certificats utilise le mot de passe :

   ```
   export ROOTCAPASS="placez_votre_mot_de_passe_ici"
   /opt/ibm/ccm/create_security_artifacts.sh -genrootca -workdir
   "${KEYFILES_DIR}" -keyalg EC -hostname
   APM_MIN_server -dname "APM_Root_CA" -label "Root_CA_Cert"
   ```

   Important : Pour les étapes 2, 3 et 4, vous pouvez remplacer le libellé de clé. Les libellés suivants ne sont utilisés comme exemples que dans ces étapes :

   - Root_CA_Cert
   - Certificat_agent_APM
   - server_key

   Vous pouvez remplacer le nom d'hôte par un nom d'hôte défini par l'utilisateur.

Une fois que vous avez terminé, vous supprimez le mot de passe de la variable d'environnement : entrez **export -n ROOTCAPASS**. L'autorité de certification racine est créée dans le répertoire "${KEYFILES_DIR}"/apmCA. Ce dernier contient deux sous-répertoires : keyfiles et exports. Le sous-répertoire keyfiles/ contient le magasin de clés de l'autorité de certification racine et le sous-répertoire exports/, le certificat public de l'autorité de certification racine.

3. Pour créer le magasin de clés de l'agent et une demande de signature de certificat, vous devez spécifier un nom générique comme nom d'hôte. Vous n'avez pas besoin d'utiliser le nom d'hôte default.agent. Le certificat est utilisé par tous les agents qui communiquent avec un serveur spécifique. Vous devez créer un mot de passe pour le magasin de clés de l'agent et une clé privée à exporter dans l'environnement avant d'exécuter le script :

   ```
   export APMPASS="placez_votre_mot_de_passe_magasin_de_clés_agent_ici"
   /opt/ibm/ccm/create_security_artifacts.sh -gencsr -workdir "${KEYFILES_DIR}"
   -keyalg EC -hostname default.agent -dname "APM_Root_CA" -label
   "Certificat_agent_APM"
   ```

   Un message contenant le chemin d'accès au fichier CSR est affiché sur la console. Une fois que vous avez terminé, vous devez supprimer le mot de passe de la variable d'environnement : **export -n APMPASS**.

4. Pour créer un magasin de clés de serveur et une demande de signature de certificat, vous devez spécifier l'option **hostname name to -hostname**. Il peut s'agir d'un nom d'hôte générique ou d'un nom d'hôte réel du serveur. Vous devez définir le mot de passe du magasin de clés du serveur et la clé privée.

   ```
   export APMPASS="placez_votre_mot_de_passe_magasin_de_clés_serveur_ici"
   /opt/ibm/ccm/create_security_artifacts.sh -gencsr -workdir "${KEYFILES_DIR}"
   -keyalg EC -hostname default.server -dname "APM_Root_CA" -label "server_key"
   ```

   Un message contenant le chemin d'accès au fichier CSR est affiché sur la console. Une fois que vous avez terminé, vous devez supprimer le mot de passe de la variable d'environnement : **export -n APMPASS**.

5. Signez la demande de signature de certificat de l'agent à l'aide de l'autorité de certification racine que vous avez créée à l'étape 2. Le certificat de l'agent signé par le magasin de clés de l'agent et le certificat public de l'autorité de certification racine sont alors ajoutés automatiquement au magasin de clés de l'agent :

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -signcsr -keyalg EC -rootcakdb
   "${KEYFILES_DIR}"/apmCA/keyfiles/keyfile.kdb -rootcalabel "Root_CA_Cert"
   -csrfile
   "${KEYFILES_DIR}"/default.agent/exports/default.agent.arm
   ```

   Important : Dans les étapes 5 et 6, -rootcalabel doit correspondre au libellé spécifié à l'étape 2.

6. Signez la demande de signature de certificat du serveur. Le certificat signé du serveur et le certificat public de l'autorité de certification racine sont ensuite ajoutés automatiquement au magasin de clés du serveur :

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -signcsr -keyalg EC -rootcakdb
   "${KEYFILES_DIR}"/apmCA/keyfiles/keyfile.kdb -rootcalabel "Root_CA_Cert"
   -csrfile
   "${KEYFILES_DIR}"/default.server/exports/default.server.arm
   ```

7. Ajoutez la clé publique de l'agent au magasin de clés du serveur. Le serveur **MIN** est configuré pour n'accepter que les connexions des clients ou des agents qui s'authentifient avec un certificat connu.

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb
   "${KEYFILES_DIR}"/default.server/keyfiles/keyfile.kdb
   -importfile "${KEYFILES_DIR}"/default.agent/exports/default.agent.cer
   -label "Certificat_agent_APM"
   ```

8. Ajoutez la clé publique du serveur au magasin de clés de l'agent pour que l'agent puisse authentifier le serveur :

```
/opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb
"${KEYFILES_DIR}"/default.agent/keyfiles/keyfile.kdb -importfile
"${KEYFILES_DIR}"/default.server/exports/default.server.cer -label "server_key"
```

9. Convertissez le magasin de clés du serveur du format GSKit (*.kdb) au format de magasin de clés Java (*.jks). Vous devez définir le mot de passe du magasin de clés du serveur :

   ```
   export APMPASS="placez_votre_mot_de_passe_magasin_de_clés_serveur_ici"
   /opt/ibm/ccm/create_security_artifacts.sh -kdb2jks -sourcekdb
   "${KEYFILES_DIR}"/default.server/keyfiles/keyfile.kdb
   ```

   Le fichier ${KEYFILES_DIR}"/default.server/keyfiles/keyfile.jks" est créé. Une fois que vous avez terminé, vous devez supprimer le mot de passe de l'environnement : **export -n APMPASS**.

10. Convertissez le magasin de clés de l'agent du format GSKit (*.kdb) au format de magasin de clés Java (*.jks). Vous devez définir le mot de passe du magasin de clés de l'agent :

    ```
    export APMPASS= "put_your_agent_keystore_password_here"
    /opt/ibm/ccm/create_security_artifacts.sh -kdb2jks -sourcekdb
    "${KEYFILES_DIR}"/default.agent/keyfiles/keyfile.kdb
    ```

    Une fois que vous avez terminé, vous devez supprimer le mot de passe de l'environnement : **export -n APMPASS**.

11. Copiez les fichiers de clés créés dans le répertoire keyfiles principal :

    ```
    /bin/cp "${KEYFILES_DIR}"/default.agent/keyfiles/keyfile.* /opt/ibm/ccm/
    keyfiles/
        /bin/cp "${KEYFILES_DIR}"/default.agent/keyfiles /KAES256.ser /opt/ibm/ccm/
    keyfiles/
        /bin/cp "${KEYFILES_DIR}"/default.server/keyfiles/keyfile.jks /opt/ibm/ccm/
    keyfiles/server.jks
    ```

12. Copiez le fichier server.jks dans l'emplacement du serveur Liberty. Pour que les communications de l'agent soient sécurisées, utilisez le serveur **min** :

    ```
    /bin/cp /opt/ibm/ccm/keyfiles/server.jks /opt/ibm/wlp/usr/
    servers/min/resources/security/key.jks
    ```

    Si vous avez précédemment ajouté un certificat d'autorité de certification dans le fichier key.jks pour réacheminer des événements via une connexion SSL à votre serveur SMTP, vous devez le rajouter dans le nouveau magasin de clés. Pour des instructions, voir Gestionnaire d'événements dans «Configuration avancée», à la page 1117.

13. Codez le mot de passe du magasin de clés du serveur (xor) :

    ```
    /opt/ibm/wlp/bin/securityUtility encode
    ```

14. Copiez l'élément XML keyStore qui contient la définition "defaultKeyStore" du magasin de clés de *rép_install*/wlp/usr/servers/min/server.xml vers *rép_install*/wlp/usr/servers/min/user-exit.xml s'il n'existe pas déjà dans le fichier user-exit.xml. (user-exit.xml est un fichier de remplacement pour server.xml). Remplacez l'entrée password dans user-exit.xml par le mot de passe que vous venez de coder à l'étape 13. Supprimez l'élément XML keyStore du fichier server.xml.

15. Copiez l'élément XML ssl qui contient l'attribut enabledCiphers du fichier *rép_install*/wlp/usr/servers/min/server.xml vers le fichier *rép_install*/wlp/usr/servers/min/user-exit.xml s'il n'existe pas déjà dans le fichier user-exit.xml. Ajoutez ensuite la ligne clientAuthentication="true" après la ligne enabledCiphers dans le fichier user-exit.xml. Supprimez l'élément XML ssl du fichier server.xml.

16. Si vous avez modifié les libellés de clé aux étapes 3 et 4 (en remplaçant l'argument par une option **-label**), éditez les valeurs des attributs serverKeyAlias et clientKeyAlias dans le fichier user-exit.xml comme suit :

    ```
    serverKeyAlias="placez_libellé_clé_serveur_ici"
    clientKeyAlias="placez_libellé_clé_agent_ici"
    ```

Remarque : Si les entrées d'alias de clé "serverKeyAlias" et "clientKeyAlias" n'existent pas dans le fichier server.xml, vous devez ajouter dans user-exit.xml les entrées à la section <ssl>, après la propriété "enabledCiphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256".

17. Redémarrez le serveur **min** :

    ```
    apm stop min
    apm start min
    ```

18. Si la Passerelle hybride d'IBM Cloud Application Performance Management est installée dans votre environnement Tivoli Monitoring, copiez le magasin de clés de l'agent JKS dans l'emplacement de la Passerelle hybride :

    ```
    cp /opt/ibm/ccm/keyfiles/keyfile.* /opt/ibm/wlp/usr/servers
    /hybridgateway/resources/security/
    ```

19. Selon que vous avez ou non installé des agents, effectuez l'une des étapes suivantes :
    - Si vous avez installé des agents, copiez les fichiers de clés dans le répertoire d'installation des agents : `cp "/opt/ibm/ccm/keyfiles/keyfile.* chemin_images_agents/keyfiles."`.
      – Modifiez le fichier de configuration de l'agent pour indiquer le certificat à utiliser par l'agent. La variable suivante doit être modifiée ou ajoutée au fichier de configuration :

        KDEBE_KEY_LABEL="*libellé_clé_agent*"

        Par exemple, KDEBE_KEY_LABEL="*Certificat_agent_APM*"

        - Pour une installation Windows 64 bits, modifiez la variable dans le fichier \TMAITM6_x64\K*CP*ENV, où *CP* correspond au code produit de l'agent.
        - Pour une installation Windows 32 bits, modifiez la variable dans le fichier \TMAITM6\K*CP*ENV, où *CP* correspond au code produit de l'agent.

        Par exemple, pour un agent installé dans C:\IBM\APM, pour modifier la configuration de l'agent de système d'exploitation sur une installation 64 bits, vous devez modifier le fichier suivant : C:\IBM\APM\TMAITM6_x64\KNTENV.

        - Sous Linux/AIX, modifiez la variable dans le fichier suivant : *chemin_installation_agent*/config/global.environment.

      – Redémarrez les agents.
    - Si vous n'avez pas installé d'agents, utilisez l'outil de configuration des agents pour modifier les images d'agent afin qu'elles contiennent les nouveaux certificats.
      a. Pour créer les modules de configuration, utilisez l'outil /opt/ibm/ccm/make_configuration_packages.sh, y compris le paramètre **-k** pour indiquer l'emplacement des fichiers de clés d'agent. Pour plus d'informations, voir l'étape 2, à la page 163 dans «Configuration des images téléchargées», à la page 162.
      b. Pour configurer les images d'agent, utilisez le script /opt/ibm/ccm/configure_agent_images.
      c. Décompressez l'image d'agent obtenue et modifiez le fichier de configuration pour indiquer le certificat à utiliser par les agents :
        – La variable *KDEBE_KEY_LABEL* = **libellé_clé_agent** doit être ajoutée aux fichiers de configuration dans une image d'agent décompressée :

          Par exemple, *KDEBE_KEY_LABEL*=**"Certificat_agent_APM"**.

        – Sous Linux/AIX, modifiez la variable dans le fichier suivant : *chemin_image_agent_décompressée*/.apm_config/agent_global.environment.

          Par exemple, APM_Agent_Install_8.1.4.0/.apm_config/agent_global.environment.

        – Sous Windows, modifiez la variable dans la section [CMA_CONFIG_VARIABLES] du fichier suivant : *chemin_image_agent_décompressée*\apm_config\framework_silent_install.txt.
        – Compressez l'image d'installation de l'agent décompressée.

      Le module de configuration des agents que vous avez créé à l'aide du script make_configuration_packages.sh contient également le module Windows avec les données de configuration et le script Windows.

Que faire ensuite

Vous devez configurer les agents du serveur Cloud APM pour utiliser le protocole HTTPS et les certificats. Pour obtenir des instructions, voir «Configuration du protocole de communications pour les agents de serveur», à la page 1097.

Configuration d'un certificat personnalisé d'une autorité de certification racine tierce pour les communications d'agent HTTPS

Lorsque le serveur Cloud APM est installé, un ensemble de certificats signés utilisés par le serveur Cloud APM et les agents est créé. Si votre règle de sécurité locale l'exige, vous pouvez utiliser les certificats émis par votre autorité de certification tierce.

Avant de commencer

Vérifiez que les pare-feux ou les périphériques de filtrage réseau qui se trouvent entre le serveur Cloud APM et les agents autorisent les communications sur le port **443**.

Pourquoi et quand exécuter cette tâche

Vous devez créer un ensemble de fichiers de magasin de clés contenant des clés de chiffrement et des certificats : un ensemble pour le serveur Cloud APM et un autre pour les agents. Vous devez préparer deux mots de passe : un pour le magasin de clés du serveur Cloud APM et l'autre pour celui des agents. Dans les exemples suivants, les mots de passe de la base de données du fichier de clés des agents et du serveur sont les mêmes. Les exemples utilisent les valeurs suivantes :

- Répertoire d'installation : `/opt/ibm`
- Nom d'hôte du serveur Cloud APM : `serverhostname`
- Répertoire de travail du magasin de clés : `/opt/ibm/ccm/keyfiles`

Procédure

Si vous souhaitez utiliser un certificat généré par une autorité de certification tierce, procédez comme suit :

1. Connectez-vous au serveur Cloud APM et créez votre propre répertoire de travail de magasin de clés sous `/opt/ibm/ccm` (par exemple, `/opt/ibm/ccm/working_directory`). Vous pouvez également utiliser le répertoire `/opt/ibm/ccm/keyfiles` existant et préserver l'aspect unique de vos répertoires de fichier de clés en sélectionnant des paramètres **hostname** autres que **default.server**, **default.agent** et **apmCA**. Ces répertoires de travail sont utilisés par le programme d'installation pour créer des fichiers de clés de certificat autosigné utilisés par défaut. La valeur de **hostname** est utilisée en tant que nom du sous-répertoire pour stocker les fichiers de clés. Cette valeur est indiquée dans le fichier `create_security_artifacts.sh`.

   Lors de la réinstallation du serveur Cloud APM, si le programme d'installation trouve un répertoire `/opt/ibm/ccm/keyfiles` existant, il ne remplace pas les fichiers de clés dans ce répertoire. Toutefois, si un répertoire autre que `/opt/ibm/ccm/keyfiles` a été utilisé lors de l'installation précédente, les fichiers de clés sont alors remplacés. Par exemple, si vous avez utilisé un sous-répertoire de `/keyfiles`, ces fichiers de clés sont remplacés lors de la réinstallation.

   Au cours des étapes suivantes, le script **create_security_artifacts.sh** crée une demande de signature de certificat (CSR) dans le répertoire *répertoire_de_travail*`/exports` sous la forme d'un fichier `.arm`. Vous devez envoyer le fichier `.arm` à votre autorité de certification tierce pour signature. Cette dernière renvoie votre nouveau certificat, le certificat d'émetteur et tout autre certificat dans la chaîne de confiance du certificat d'émetteur.

   Le script **create_security_artifacts.sh** crée également un ensemble de fichiers dans le répertoire *répertoire_de_travail*`/keyfiles` qui doivent être mis à jour lorsque vous obtenez vos certificats de l'autorité de certification tierce et les importez dans le magasin de clés. Ces fichiers doivent être conservés.

2. Pour créer le magasin de clés de l'agent et la demande de signature de certificat, définissez d'abord la variable d'environnement APMPASS sur le mot de passe du magasin de clés. Cette variable est utilisée par le script **create_security_artifacts.sh**. Exemple :

   ```
   export APMPASS="placez_votre_mot_de_passe_magasin_de_clés_agent_ici"
   ```

3. Créez le magasin de clés de l'agent et la demande de signature de certificat. Le certificat d'agent étant utilisé par l'ensemble des agents, vous devez créer un **hostname** générique à l'aide du nom d'hôte du serveur Cloud APM. Il est recommandé d'incorporer le paramètre **hostname** du serveur Cloud APM pour faciliter l'identification. La valeur utilisée pour le paramètre **hostname** forme le nom du sous-répertoire sous */répertoire_de_travail* dans lequel le magasin de clés de l'agent et les demandes de signature de certificat sont créés.

   Dans les exemples suivants, la variable **hostname** du serveur Cloud APM est définie sur **serverhostname**.

   Définissez le paramètre **dname** sur un nom standard x509 identifiant votre domaine. Par exemple,

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -gencsr -workdir /opt/ibm/ccm/keyfiles
   -keyalg EC -hostname serverhostname.agent
   -dname OU=ou,O=o,L=l,ST=st,C=c -label APM_Agent_Certificate
   ```

   Vous recevez le message suivant :

   ```
   La demande de signature de certificat a été créée et est disponible dans le fichier suivant :
   /opt/ibm/ccm/keyfiles/serverhostname.agent/exports/serverhostnameagent.arm
   Envoyez-la à votre autorité de certification pour signature.
   ```

4. Si le mot de passe du magasin de clés du serveur est différent du mot de passe de l'agent, annulez la définition de la variable APMPASS et exportez-la de nouveau à l'aide du mot de passe du serveur. Exemple :

   ```
   export -n APMPASS
   ```

   ```
   export APMPASS="placez_votre_mot_de_passe_magasin_de_clés_serveur_ici"
   ```

5. Créez le magasin de clés du serveur et la demande de signature de certificat :

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -gencsr -workdir /opt/ibm/ccm/keyfiles
   -keyalg EC -hostname serverhostname
   -dname OU=ou,O=o,L=l,ST=st,C=c -label APM_Server_Certificate
   ```

   Vous recevez le message suivant :

   ```
   La demande de signature de certificat a été créée et est disponible dans le fichier suivant :
   /opt/ibm/ccm/keyfiles/serverhostname/exports/myhost.com.arm
   Envoyez-la à votre autorité de certification pour signature.
   ```

   La création des demandes de signature de certificat entraîne la création d'une clé privée initialement disponible dans le fichier *répertoire_de_travail*/keyfiles/keyfile.rdb. Cette clé est transférée ultérieurement dans le fichier keyfile.kdb lors de l'importation du certificat. Tous les autres fichiers de clés doivent rester dans le répertoire *répertoire_de_travail*/keyfiles/ car ils sont utilisés lors des étapes suivantes, même si vous spécifiez uniquement le chemin d'accès au fichier keyfile.kdb.

   L'autorité de certification personnalisée doit utiliser un chiffrement compatible avec la norme de sécurité Suite-B. La suite de chiffrement suivante est acceptée par le serveur Cloud APM : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. Vous devez vous assurer que tous les certificats de la chaîne de confiance contiennent le paramètre **namedCurve** avec le nom de la courbe utilisée pour la signature : (rfc 5480 section 2.1.1 states that implicitCurve and specifiedCurve must not be used in PKIX).

   Par défaut, les agents de surveillance sont configurés pour utiliser le mode FIPS. Par conséquent, l'autorité de certification tierce doit signer votre certificat à l'aide d'un algorithme ECDSA (Elliptic Curve Digital Signature Algorithm). Si l'autorité de certification tierce fournit uniquement une signature RSA, vous ne pourrez utiliser le nouveau certificat qu'après la mise en commentaire de l'instruction KDEBE_FIPS_MODE_ENABLED=SuiteB-128 de l'agent. Editez les commandes suivantes :

   - Linux AIX

rép_install/config/global.environment file:#KDEBE_FIPS_MODE_ENABLED=SuiteB-128

- Windows

rép_install/tmaitm6_x64/k*cp*cma.ini file. ;-- KDEBE_FIPS_MODE_ENABLED=SuiteB-128

où *cp* correspond au code produit de l'agent.

6. Envoyez les fichiers CSR à l'autorité de certification tierce privée pour signature. Copiez tous les certificats que vous recevez pour le serveur et l'agent dans le répertoire *répertoire_de_travail*/exports, ceci à des fins de stockage.
   a. Copiez les certificats de serveur, de signataire et racine dans le répertoire suivant : /opt/ibm/ccm/keyfiles/serverhostname/exports
   b. Copiez les certificats d'agent, de signataire et racine dans le répertoire suivant : /opt/ibm/ccm/keyfiles/serverhostname.agent/exports

   Si vous utilisez des certificats pendant un bref laps de temps uniquement, par exemple, lorsque vous attendez que votre autorité de certification crée des certificats, annulez la définition de la variable APMPASS ou fermez votre session. Cela permet de supprimer le mot de passe de l'environnement. Assurez-vous que la variable d'environnement APMPASS est correctement définie lorsque vous exécutez le script create_security_artifacts.sh.
7. Ajoutez le certificat racine de votre autorité de certification tierce aux fichiers keystore.kdb des agents et du serveur, sauf s'il constitue également le certificat de signataire. Si votre chaîne de confiance ne contient qu'un seul certificat, le certificat de signataire est le certificat racine. Vous pouvez alors ignorer cette étape.

   /opt/ibm/ccm/create_security_artifacts.sh –addkeytodb -destkdb
   répertoire_de_travail/keyfiles/keyfile.kdb -importfile
   chemin_cert_racine_de_votre_autorité_certification -label *libellé_racine_de_votre_autorité_certification*
   a. Exemple pour l'agent :

      /opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb
      /opt/ibm/ccm/cust_certs/custom.agent/keyfiles/keyfile.kdb -importfile
      /opt/ibm/ccm/keyfiles/serverhostname.agent/exports/rootca.crt -label RootCA

      Vous recevez le message suivant :

      L'ajout du certificat a abouti.
   b. Exemple pour le serveur :

      /opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb
      /opt/ibm/ccm/keyfiles/myhost.com/keyfiles/keyfile.kdb -importfile
      /opt/ibm/ccm/keyfiles/serverhostname/exports/rootca.crt -label RootCA

      Vous recevez le message suivant :

      L'ajout du certificat a abouti.
8. (Facultatif) Ajoutez le certificat intermédiaire de votre autorité de certification tierce autre que le certificat d'émetteur (signataire) :

   /opt/ibm/ccm/create_security_artifacts.sh -addkeytodb
   -destkdb working_directory/keyfiles/keyfile.kdb
   -importfile *chemin_cert_intermédiaire_de_votre_autorité_certification* -label *libellé_intermédiaire_de_votre_autorité*

   Répétez cette étape pour tous les certificats intermédiaires fournis par votre autorité de certification tierce autres que le certificat d'émetteur.
9. Importez votre nouveau certificat et le certificat de signataire. Cette commande est inhabituelle car elle utilise **rootca** pour les noms de paramètre du signataire, et les certificats de l'autorité de certification racine ne sont généralement pas les signataires lorsqu'une autorité de certification tierce privée émet vos certificats.

```
/opt/ibm/ccm/create_security_artifacts.sh -importcert
-rootcacert chemin_accès_certificat_d'émetteur_autorité_certification
-rootcalabel libellé_certificat_d'émetteur
-destkdb répertoire_de_travail/nom_d'hôte/keyfiles/keyfile.kdb
-importfile chemin_accès_nouveau_certificat_signé
```

a. Ajoutez votre nouveau certificat de serveur au fichier keystore.kdb du serveur :

```
/opt/ibm/ccm/create_security_artifacts.sh -importcert
-importfile /opt/ibm/ccm/keyfiles/serverhostname/exports/server.crt
-rootcacert /opt/ibm/ccm/keyfiles/serverhostname/exports/signca.crt
-destkdb /opt/ibm/ccm/keyfiles/serverhostname/keyfiles/keyfile.kdb -rootcalabel "SignerCA"
```

Vous recevez le message suivant :

```
Importation du certificat réussie.
```

b. Ajoutez votre nouveau certificat d'agent au fichier keystore.kdb de l'agent :

```
/opt/ibm/ccm/create_security_artifacts.sh -importcert
-importfile /opt/ibm/ccm/keyfiles/serverhostname.agent/exports/agent.crt
-rootcacert /opt/ibm/ccm/keyfiles/serverhostname.agent/exports/signca.crt
-destkdb /opt/ibm/ccm/keyfiles/servehostname.agent/keyfiles/keyfile.kdb
-rootcalabel "SignerCA"
```

Vous recevez le message suivant :

```
Importation du certificat réussie.
```

10. Ajoutez le certificat d'agent au magasin de clés du serveur. Le serveur Cloud APM est configuré pour n'accepter que les connexions des clients ou des agents qui s'authentifient avec un certificat connu.

```
/opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb
 /opt/ibm/ccm/keyfiles/serverhostname/keyfiles/keyfile.kdb
 -importfile /opt/ibm/ccm/keyfiles/serverhostname.agent/exports
/serverhostname.agent.crt -label "APM_Agent_Certificate"
```

11. Ajoutez le certificat de serveur au magasin de clés de l'agent pour que l'agent puisse s'authentifier sur le serveur :

```
/opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb
/opt/ibm/ccm/keyfiles/serverhostname.agent/keyfiles/keyfile.kdb
 -importfile /opt/ibm/ccm/keyfiles/serverhostname/exports
/serverhostname.crt -label "APM_Server_Certificate"
```

12. Convertissez les magasins de clés de l'agent et du serveur du format GSKit (*.kdb) au format de magasin de clés Java™ (*.jks). Exemple d'agent :

```
/opt/ibm/ccm/create_security_artifacts.sh -kdb2jks -sourcekdb
 /opt/ibm/ccm/keyfiles/serverhostname.agent/keyfiles/keyfile.kdb
```

Le fichier /opt/ibm/ccm/keyfiles/serverhostname.agent/keyfiles/keyfile.jks est créé. Exemple de serveur :

```
/opt/ibm/ccm/create_security_artifacts.sh -kdb2jks -sourcekdb
 /opt/ibm/ccm/keyfiles/serverhostname/keyfiles/keyfile.kdb
```

Le fichier /opt/ibm/ccm/keyfiles/serverhostname/keyfiles/keyfile.jks est créé.

13. Supprimez le mot de passe du magasin de clés de l'environnement :

```
export -n APMPASS
```

14. Les fichiers de clés utilisés par le serveur Cloud APM pour la communication d'agent se trouvent dans le répertoire /opt/ibm/wlp/usr/server/min/resources/security. Sauvegardez le fichier key.jks qui s'y trouve déjà et remplacez-le par la nouvelle version.

```
cp /opt/ibm/wlp/usr/servers/min/resources/security/key.jks
/opt/ibm/wlp/usr/servers/min/resources/security/key.jks.orig
cp /opt/ibm/ccm/keyfiles/serverhostname/keyfiles/keyfile.jks
/opt/ibm/wlp/usr/servers/min/resources/security/key.jks
```

Si vous avez précédemment ajouté un certificat d'autorité de certification tierce au fichier `key.jks` pour réacheminer des événements utilisant une connexion SSL à votre serveur SMTP, vous devez le rajouter au nouveau magasin de clés. Pour des instructions, voir Gestionnaire d'événements dans Configuration avancée.

15. Codez le mot de passe du magasin de clés du serveur (xor) :

    ```
    /opt/ibm/wlp/bin/securityUtility encode
    ```

16. Copiez l'élément xml keyStore qui contient la définition "defaultKeyStore" du magasin de clés de *rép_install*`/wlp/usr/servers/min/server.xml` dans *rép_install*`/wlp/usr/servers/min/user-exit.xml` s'il n'existe pas déjà dans le fichier `user-exit.xml`. (`user-exit.xml` est un fichier de remplacement pour `server.xml`.) Remplacez la valeur de l'attribut password dans `user-exit.xml` par le mot de passe que vous venez de coder à l'étape 15. Supprimez l'élément XML keyStore du fichier `server.xml`.
17. Copiez l'élément xml ssl qui contient l'attribut enabledCiphers du fichier *rép_install*`/wlp/usr/servers/min/server.xml` dans le fichier *rép_install*`/wlp/usr/servers/min/user-exit.xml` . Ajoutez ensuite la ligne `clientAuthentication="true"` après la ligne enabledCiphers dans le fichier `user-exit.xml`. Supprimez l'élément XML ssl du fichier `server.xml`.
18. Mettez à jour les libellés de certificat dans le fichier *rép_install*`/wlp/usr/servers/min/user-exit.xml` du serveur Cloud APM et éditez-les comme suit :

    ```
    serverKeyAlias="APM_Server_Certificate"
    clientKeyAlias="APM_Agent_Certificate"
    ```

    Si les entrées d'alias de clé serverKeyAlias et clientKeyAlias ne figurent pas dans le fichier `user-exit.xml` , vous devez les ajouter à la section <ssl> après l'attribut enabledCiphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256.
19. Redémarrez le serveur Cloud APM :

    ```
    apm stop min
    apm start min
    ```

20. Si la Passerelle hybride est installée dans votre environnement Tivoli Monitoring, copiez le magasin de clés de l'agent JKS dans l'emplacement de la passerelle hybride :

    ```
    /opt/ibm/wlp/usr/servers/hybridgateway/resources/security/
    ```

21. Pour installer les fichiers de clés des agents, selon que vous avez ou non installé des agents, effectuez l'une des étapes suivantes :
    - Si vous avez installé des agents, copiez les fichiers de clés dans les systèmes d'agent, éditez le fichier de configuration des agents, puis redémarrez les agents :
      a. Copiez le contenu du répertoire `/opt/ibm/ccm/keyfiles/serverhostname.agent/keystore` dans le répertoire `/opt/ibm/ccm/keyfiles` sur tous les systèmes d'agent.
      b. Modifiez le fichier de configuration des agents pour indiquer le certificat à utiliser par l'agent. Pour ce faire, éditez ou ajoutez la variable suivante :

         ```
         KDEBE_KEY_LABEL="Certificat_agent_APM"
         ```

         Le fichier de configuration des agents que vous éditez dépend de votre système d'exploitation :

         – Linux AIX

           ```
           /chemin_installation_agent/config/global.environment
           ```

         – Windows

           ```
           64 bits\TMAITM6_x64\KPCENV
           ```

         – Windows

           ```
           32 bits\TMAITM6\KCPENV
           ```

           où *CP* correspond au code produit. Par exemple, pour un agent installé dans `C:\IBM\APM`, pour modifier la configuration de l'agent de système d'exploitation sur une installation 64 bits, vous devez modifier le fichier suivant : `C:\IBM\APM\TMAITM6_x64\KNTENV`.

c. Redémarrez les agents.

Avant de pouvoir installer les agents, vous devez configurer les images d'installation téléchargées pour initier la communication avec le serveur Cloud APM. Si vous n'avez pas sélectionné l'option de configuration des images téléchargées lors de l'installation du serveur, vous pouvez modifier le fichier de configuration afin d'indiquer le certificat à utiliser par les agents. La variable `KDEBE_KEY_LABEL = libellé_clé_agent` doit être ajoutée aux fichiers de configuration dans une image d'agent décompressée. Par exemple,

```
KDEBE_KEY_LABEL="Certificat_agent_APM"
```

– Linux AIX

chemin_image_agent_décompressée/.apm_config/agent_global.environment

Par exemple, APM_Agent_Install_8.1.4/.apm_config/agent_global.environment

– Windows Modifiez la variable dans la section CMA_CONFIG_VARIABLES du fichier suivant :

chemin_image_agent_décompressée\apm_config\framework_silent_install.txt

- Si vous n'avez pas installé d'agents, utilisez l'outil de configuration des agents pour modifier les images d'agent afin qu'elles contiennent les nouveaux certificats.
  a. Pour créer les modules de configuration, utilisez l'outil /opt/ibm/ccm/make_configuration_packages.sh, y compris le paramètre **-k** pour indiquer l'emplacement des fichiers de clés d'agent. Pour plus d'informations, voir l'étape 2, à la page 163 dans «Configuration des images téléchargées», à la page 162.
  b. Pour configurer les images d'agent, utilisez le script /opt/ibm/ccm/configure_agent_images.
  c. Décompressez l'image d'agent obtenue et modifiez le fichier de configuration pour indiquer le certificat à utiliser par les agents :
     – La variable *KDEBE_KEY_LABEL* = **libellé_clé_agent** doit être ajoutée aux fichiers de configuration dans une image d'agent décompressée :

       Par exemple, *KDEBE_KEY_LABEL*=**"Certificat_agent_APM"**.
     – Sous Linux/AIX, modifiez la variable dans le fichier suivant : *chemin_image_agent_décompressée*/.apm_config/agent_global.environment.

       Par exemple, APM_Agent_Install_8.1.4.0/.apm_config/agent_global.environment.
     – Sous Windows, modifiez la variable dans la section [CMA_CONFIG_VARIABLES] du fichier suivant : *chemin_image_agent_décompressée*\apm_config\framework_silent_install.txt.
     – Compressez l'image d'installation de l'agent décompressée.

  Le module de configuration des agents que vous avez créé à l'aide du script make_configuration_packages.sh contient également le module Windows avec les données de configuration et le script Windows.

Que faire ensuite

Vous devez configurer les agents du serveur Cloud APM pour utiliser le protocole HTTPS et les certificats. Pour obtenir des instructions, voir «Configuration du protocole de communications pour les agents de serveur», à la page 1097.

Configuration des collecteurs de données

Pour afficher dans la console Cloud APM les données de surveillance concernant vos applications à l'aide d'un collecteur de données, vous devez accomplir plusieurs tâches de configuration.

Pourquoi et quand exécuter cette tâche

Cette procédure, qui inclut des étapes obligatoires, conditionnelles et facultatives, constitue un plan de configuration de la surveillance pour vos applications. Effectuez les étapes nécessaires en fonction de vos besoins.

Procédure

1. Téléchargez et configurez les images d'installation des collecteurs de données. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.
2. Si vous surveillez vos applications basées sur Liberty IBM Cloud Private, voir Configuring data collection for Java-based microservices or Liberty-based applications sur le APM Developer Center pour des informations complémentaires.
3. Configurez le collecteur de données pour qu'il collecte des données de surveillance concernant les applications IBM Cloud et sur site, puis envoyez-les au serveur Cloud APM. Effectuez une ou plusieurs des tâches suivantes en fonction du type de votre application :

   Applications Liberty
   - «Configuration du collecteur de données Liberty pour les applications sur site», à la page 813
   - «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 845

   Applications Node.js
   - «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 555
   - «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 561

   Applications Python
   - «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 624
   - «Configuration du collecteur de données Python pour les applications sur site», à la page 629

   Applications Ruby
   - «Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 677

   Applications Java
   - «Configuration de la surveillance de J2SE», à la page 418
4. Si vous êtes un utilisateur public de IBM Cloud, après avoir configuré le collecteur de données, vous devez configurer la passerelle sécurisée IBM Cloud de façon à lui permettre de se connecter au serveur Cloud APM. Pour plus d'informations, voir «Configuration de la passerelle sécurisée IBM Cloud», à la page 234.
5. Si le fichier de clés ou le serveur Cloud APM est modifié, reconnectez le collecteur de données au serveur Cloud APM. Pour plus d'informations, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 234.

Que faire ensuite

Après avoir effectué toutes les tâches de configuration nécessaires, vous pouvez vérifier que les données de surveillance relatives à votre application IBM Cloud s'affichent dans la console Cloud APM.

Configuration de la passerelle sécurisée IBM Cloud

Si vous êtes un utilisateur public de IBM Cloud et que vous souhaitez connecter le collecteur de données au serveur Cloud APM sur site, configurez la passerelle sécurisée IBM Cloud.

Pourquoi et quand exécuter cette tâche

Si le collecteur de données ne peut pas se connecter directement au serveur Cloud APM sur site, par exemple, s'il existe un pare-feu, vous devez configurer la passerelle sécurisée.

Procédure

1. Configurez la passerelle sécurisée. Pour des instructions, voir Getting started with the Secure Gateway.

   Important : L'hôte où vous installez Secure Gateway Client doit disposer d'une connectivité réseau avec votre serveur Cloud APM local.
2. Cliquez sur **Secure Gateway** dans la liste des services de l'application pour ouvrir l'interface utilisateur de Secure Gateway.
3. Dans l'interface utilisateur de Secure Gateway, définissez les variables suivantes pour ajouter une destination :
   a. Définissez la valeur de **Resource Hostname** sur le nom d'hôte de l'hôte du serveur Cloud APM (tel que vous le voyez dans votre réseau local).
   b. Affectez à **Resource Port** la valeur `80`.
   c. Affectez à **Protocol** la valeur `HTTP`.

   Lorsque vous sauvegardez la destination, Secure Gateway affecte une valeur **Cloud Host : Port** pour la destination, qui est requise à l'étape 5.
4. Dans le tableau de bord IBM Cloud de l'application, cliquez sur **Variables d'environnement** > **USER-DEFINED** et ajoutez une variable intitulée *APM_BM_GATEWAY_URL*.
5. Définissez la valeur de la variable *APM_BM_GATEWAY_URL* au format suivant :

   `http://`*`hôte_cloud`*`:`*`valeur_port_votre_destination`*

   Par exemple :

   `APM_BM_GATEWAY_URL=http://cap-sg-stage-2.integration.ibmcloud.com:15450`
6. Démarrez le client Secure Gateway. Consultez le fichier journal du client pour vous assurer qu'il n'y a aucun message d'erreur indiquant un éventuel problème de configuration ou de communication.

Résultats

Le collecteur de données est connecté au serveur Cloud APM sur site.

Reconnexion du collecteur de données au serveur Cloud APM

Si le serveur Cloud APM, le fichier de clés ou le mot de passe du fichier de clés est modifié, vous devez définir plusieurs variables d'environnement pour reconnecter le collecteur de données au serveur Cloud APM.

Avant de commencer

Si le fichier de clés est modifié, chiffrez d'abord le mot de passe en texte normal de votre fichier de clés en Base64. Si vous êtes un utilisateur Linux, exécutez la commande suivante :

`echo -n `*`mot_de_passe_fichier_clés`*` | base64`

Le résultat de la commande est votre mot de passe chiffré. Par exemple, si votre mot de passe en texte normal est `mot de passe`, le résultat de la commande `cGFzc3dvcmQ=` est votre mot de passe chiffré. Vous

utilisez alors le mot de passe chiffré pour définir APM_KEYFILE_PSWD: *mot_de_passe_fichier_clés_chiffré* et APM_KEYFILE_PSWD=*mot_de_passe_fichier_clés_chiffré* dans les configurations ci-après.

Procédure

- Pour reconnecter les collecteurs de données au serveur Cloud APM pour les applications IBM Cloud, voir «Reconnexion des collecteurs de données pour les applications IBM Cloud».
- Pour reconnecter les collecteurs de données au serveur Cloud APM pour les applications sur site, voir «Reconnexion du collecteur de données pour les applications sur site», à la page 236.

Reconnexion des collecteurs de données pour les applications IBM Cloud

Pourquoi et quand exécuter cette tâche

Vous disposez des deux options suivantes pour reconnecter le collecteur de données au serveur Cloud APM :

- Editez le `manifest.yml` de votre application pour définir les variables.
- Définissez les variables dans l'interface utilisateur de IBM Cloud.

Procédure

- Pour utiliser le fichier `manifest.yml` de votre application IBM Cloud afin de reconnecter le collecteur de données, effectuez les étapes suivantes :
  1. Editez les variables dans le fichier `manifest.yml` de votre application IBM Cloud en fonction des modifications.
     - Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :

       ```
       APM_BM_GATEWAY_URL: http://IP_ou_nom_d'hôte_du_serveur:80
       ```

     - Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les trois variables suivantes :

       ```
       APM_BM_GATEWAY_URL: https://IP_ou_nom_d'hôte_du_serveur:443
       APM_KEYFILE_PSWD: mot_de_passe_fichier_clés_chiffré
       APM_KEYFILE_URL: http://serveur_http_hébergé:port/nom_fichier_clés
       ```

       Conseil : Le fichier de clés du collecteur de données Liberty est un fichier `.jks`. Pour les collecteurs de données Python, Node.js et Liberty, les fichiers de clés sont des fichiers `.p12`.
  2. Accédez au répertoire de votre application IBM Cloud et exécutez la commande suivante :

     ```
     cf push
     ```

- Pour utiliser l'interface utilisateur de IBM Cloud afin de reconnecter le collecteur de données, effectuez l'étape suivante :
  1. Connectez-vous à l'interface utilisateur de IBM Cloud.
  2. Cliquez sur l'application IBM Cloud.
  3. Cliquez sur **Runtime** (Exécution) dans le panneau de gauche.
  4. Accédez à l'onglet **Variable d'environnement**.
  5. Dans la section **définies par l'utilisateur**, utilisez l'une des méthodes suivantes pour définir les variables selon vos besoins :
     - Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :

       ```
       APM_BM_GATEWAY_URL: http://IP_ou_nom_d'hôte_du_serveur:80
       ```

     - Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les trois variables suivantes :

       ```
       APM_BM_GATEWAY_URL: https://IP_ou_nom_d'hôte_du_serveur:443
       APM_KEYFILE_PSWD: mot_de_passe_fichier_clés_chiffré
       APM_KEYFILE_URL: http://serveur_http_hébergé:port/nom_fichier_clés
       ```

       Conseil : Le fichier de clés du collecteur de données Liberty est un fichier `.jks`. Pour les collecteurs de données Python, Node.js et Liberty, les fichiers de clés sont des fichiers `.p12`.

6. A partir du répertoire dans lequel vous exécutez la commande **cf push** pour transmettre votre application, exécutez la commande suivante pour que vos modifications prennent effet :
   `cf restage <nom_app>`

Résultats

Les valeurs des variables sont définies correctement pour connecter le collecteur de données au serveur Cloud APM.

Reconnexion du collecteur de données pour les applications sur site

Pourquoi et quand exécuter cette tâche

En modifiant le fichier `global.environment` ou `dc.java.properties`, vous pouvez personnaliser la connexion entre le collecteur de données et le serveur Cloud APM.

Procédure

1. Recherchez le fichier correspondant qui contient les variables de connexion.
   a. Pour le collecteur de données Liberty, le collecteur de données Node.js et le collecteur de données Python, recherchez le fichier `global.environment` en fonction des informations du tableau suivant :

Nom du collecteur de données	Répertoire du fichier `global.environment`
collecteur de données Liberty	Dossier `itcamdc/etc/global.environment` dans lequel votre collecteur de données Liberty est installé.
collecteur de données Node.js	Dossier `ibmapm/etc` dans lequel votre collecteur de données Node.js est installé.
collecteur de données Python	Dossier `etc` dans lequel votre collecteur de données Python est installé.

   b. Pour le collecteur de données J2SE, recherchez le fichier `dc.java.properties` dans le dossier *DC_HOME*`/itcamdc/etc`. *DC_HOME* représente le répertoire dans lequel votre collecteur de données J2SE est installé.
2. Editez les variables dans le fichier correspondant en fonction des modifications.
   a. Pour le collecteur de données Liberty, le collecteur de données Node.js et le collecteur de données Python, éditez le fichier `global.environment` en fonction de l'instruction suivante :
      - Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :
        `APM_BM_GATEWAY_URL= http://IP_ou_nom_d'hôte_du_serveur:80`
      - Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les variables suivantes :
        ```
        APM_BM_GATEWAY_URL= https://IP_ou_nom_d'hôte_du_serveur:443
        APM_KEYFILE_PSWD=mot_de_passe_fichier_clés_chiffré
        APM_KEYFILE_URL=http://serveur_http_hébergé_:port/nom_fichier_clés
        ```

        Conseil : le fichier de clés du collecteur de données Liberty est un fichier `.jks`. Pour les collecteurs de données Python, Node.js et Liberty, les fichiers de clés sont des fichiers `.p12`.
   b. Pour le collecteur de données J2SE, éditez le fichier `dc.java.properties` en fonction de l'instruction suivante :
      - Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :
        `apm.http.type=http`

        Si la valeur de cette variable reste vide, `http` est la valeur par défaut
      - Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les variables suivantes :
        ```
        apm.ssl.password=mot_de_passe_fichier_clés_chiffré
        apm.http.type=https
        ```

Important : si le mot de passe est modifié, remplacez le fichier *DC_HOME*/itcamdc/etc/keyfile.jks par le fichier /opt/ibm/ccm/keyfiles/default.agent/keyfiles/keyfile.jks du serveur Cloud APM, *DC_HOME* correspondant au répertoire de base de votre collecteur de données J2SE.

3. Facultatif : Si vous n'utilisez pas le fichier de clés par défaut pour votre collecteur de données Node.js, définissez la variable suivante :

   ```
   APM_SNI=hôte_propriétaire_dans_le_fichier_clés
   ```

   Conseil : pour déterminer la valeur de la variable *hôte_propriétaire*, ouvrez le fichier de clés que vous utilisez et recherchez owner. Ensuite, définissez la variable *APM_SNI* sur la même valeur qu'*owner*.
4. Redémarrez l'application pour appliquer la modification.

Résultats

Les valeurs des variables sont définies correctement pour connecter le collecteur de données au serveur Cloud APM.

Exemple de fichier manifest.yml

Pour voir le contenu du fichier manifest.yml d'une application IBM Cloud, consultez les lignes suivantes :

```
applications:
- path: .
  memory: 512M
  instances: 1
  domain: mybluemix.net
  name: myBluemixApp
  host: myBluemixApp
  disk_quota: 1024M

  env:
    APM_BM_GATEWAY_URL: https://apmserver1.onprem.apm.ibmserviceengage.com
    APM_KEYFILE_PSWD: ******
    APM_KEYFILE_URL: http://samplecertapp.mybluemix.net/keyfile.p12
```

Remarque : La section env: n'est requise que si vous n'utilisez pas les paramètres par défaut pour connecter le collecteur de données au serveur Cloud APM. Spécifiez les variables répertoriées dans env: en fonction de votre situation. Pour plus d'informations, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 234.

Suppression de collecteurs de données de la console Cloud APM

Une fois que vous avez annulé la configuration d'un collecteur de données, vous devez également supprimer le collecteur de données des applications et des groupes de ressources auxquels il a été ajouté. Sinon, la console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne.

Procédure

1. Supprimez le collecteur de données des applications auxquelles vous l'avez ajouté en éditant manuellement ces applications. Cette opération est similaire à la suppression d'agents hors ligne de votre application. Voir «Affichage et suppression des agents en ligne», à la page 1151.
2. Supprimez le collecteur de données des groupes de ressources personnalisés auxquels vous l'avez ajouté. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 995.
3. Sur le serveur Cloud APM, procédez comme suit :
   a. Editez le fichier *rép_install*/serveragents/config/hostname_bi.cfg pour supprimer les lignes du collecteur de données dont la configuration a été annulée.
   b. Redémarrez le composant serveur des collecteurs de données en exécutant la commande suivante en tant que superutilisateur :

```
apm restart biagent
```

Résultats

Après quelques minutes, la console Cloud APM indique que le collecteur de données est hors ligne dans l'application **Mes composants** et dans l'interface utilisateur **Gestionnaire de groupes de ressources** si vous sélectionnez le groupe de ressources système du collecteur de données.

Une fois que l'intervalle spécifié par la propriété de configuration **Délai avant suppression d'un système hors ligne** de la page **Configuration avancée** est écoulé, le collecteur de données est automatiquement supprimé de **Mes composants** et de son groupe de ressources système.

Conseil : Vous pouvez régler le paramètre **Délai avant suppression d'un système hors ligne** au niveau de la page **Configuration avancée** pour augmenter ou réduire le délai avant suppression de l'agent hors ligne dans le cadre de la vue. Pour plus d'informations, voir «Fonction d'abonnement d'agent», à la page 1121.

A faire : Si le collecteur de données a fourni des données de suivi des transactions au serveur Cloud APM, la console Cloud APM peut continuer d'afficher le collecteur de données dans l'application **Mes composants** et afficher le message `The agent is invalid` pour le collecteur de données une fois le délai spécifié par le paramètre **Délai avant suppression d'un système hors ligne** écoulé. Si vous avez installé Cloud APM 8.1.4.0 Server, correctif temporaire 3 ou ultérieur, un collecteur de données non valide sera supprimé de l'application **Mes composants** huit jours après l'arrêt de la réception des données de suivi des transactions du collecteur de données.

Configuration de la surveillance d'Amazon EC2

L'agent Amazon EC2 permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Amazon Elastic Compute Cloud (EC2). L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement EC2. Ces mesures incluent l'utilisation de l'UC, l'utilisation d'Elastic Block Store (EBS), l'utilisation du réseau, les mises à jour de maintenance d'Amazon Web Services (AWS) et la performance des disques.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance d'Amazon EC2» pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 30.

Tableau 30. Versions d'agent

Version d'agent	Documentation
8.1.3.1, 8.1.3.2, 8.1.3.3, 8.1.3.4	Cloud APM 8.1.4

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Amazon EC2. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Amazon EC2.
- Vérifiez que les informations suivantes sont disponibles :
  - Une liste des noms de région AWS contenant les instances EC2 à surveiller.
  - Les droits de sécurité AWS (ID de clé d'accès et clé d'accès secrète) avec l'autorisation d'accès à chaque région AWS.
- Assurez-vous que les droits de sécurité AWS qui sont utilisés pour chaque région AWS sont rattachés à un groupe qui inclue au moins la règle *AmazonEC2ReadOnlyAccess*.

Pourquoi et quand exécuter cette tâche

L'agent Amazon EC2 est à la fois un agent à plusieurs instances et un agent de sous-noeud. Vous pouvez créer une instance d'agent à plusieurs sous-noeuds (une pour chaque région Amazon EC2) ou une instance d'agent pour chaque région Amazon EC2 avec un sous-noeud pour cette région. Vous pouvez également créer une combinaison de chaque type de configuration. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement. Si vous disposez de plus de 50 ressources par région Amazon EC2, nous vous suggérons de créer une instance d'agent par région, ou d'utiliser le balisage dans vos instances EC2 et de filtrer les agences d'agent selon les balises que vous créez à l'aide du paramètre de condition de filtrage de l'agent.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows».
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 243.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites.», à la page 242.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 243.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Amazon EC2 sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Amazon EC2**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple,

`ec2-inst3`.

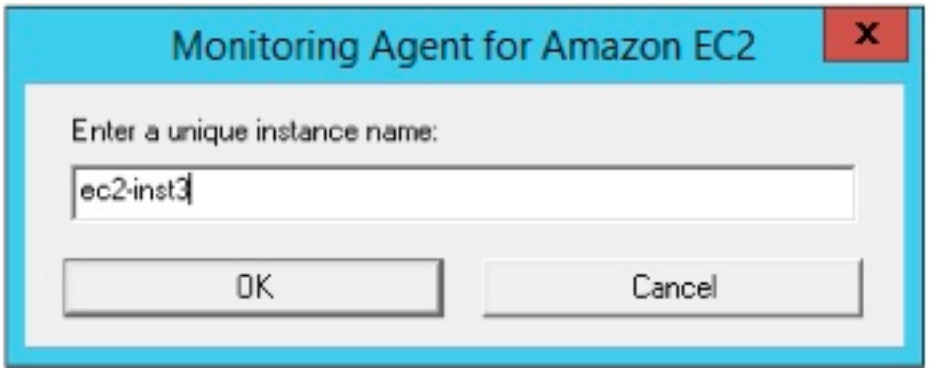


Figure 3. Fenêtre de saisie d'un nom d'instance unique.

4. Cliquez sur **Suivant** dans la fenêtre du nom d'instance de l'agent.

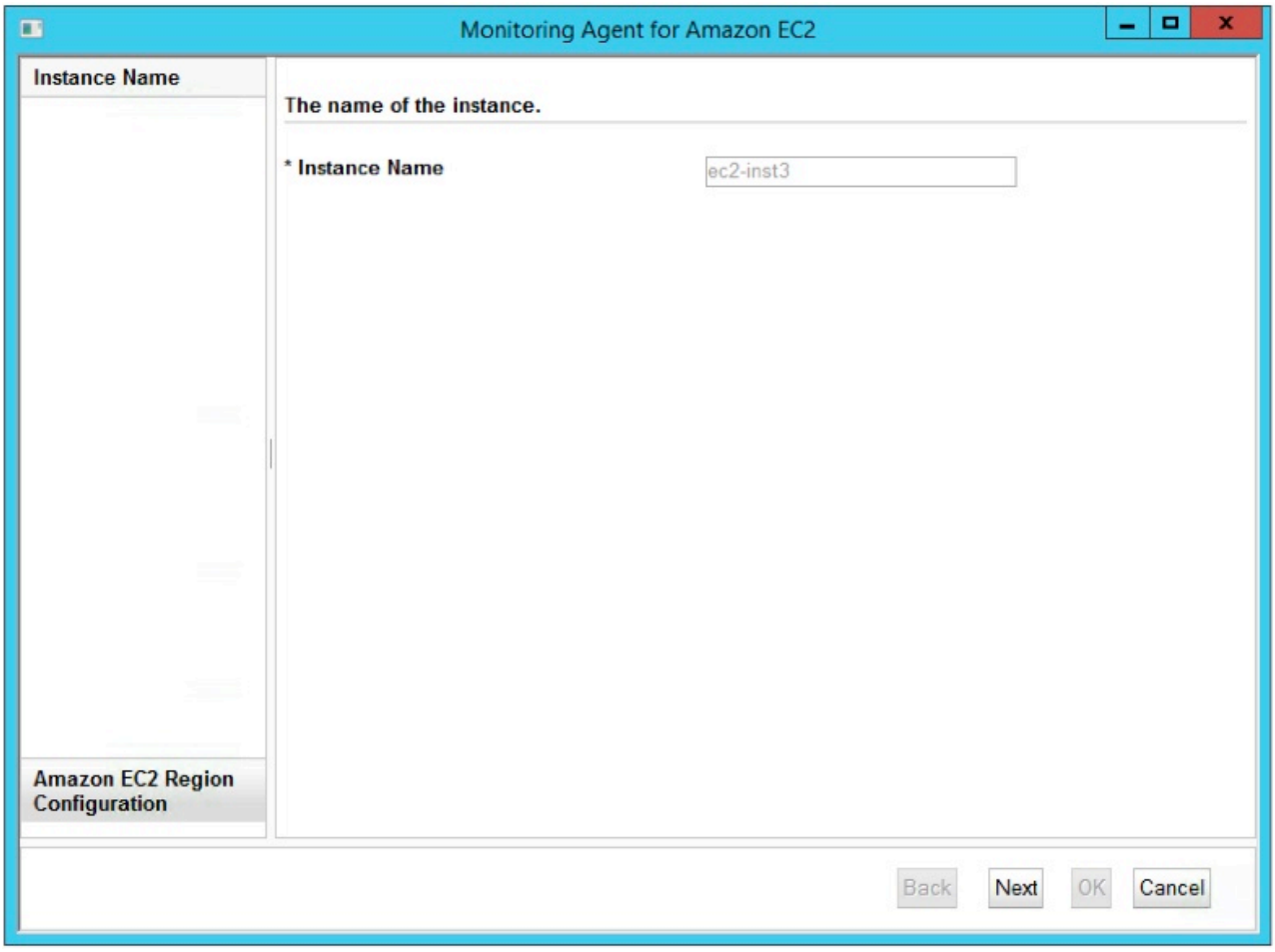


Figure 4. Fenêtre du nom d'instance de l'agent.

5. Entrez les paramètres du modèle d'instance **Amazon EC2 Region Configuration**.

   Remarque : Cette section ne décrit pas la configuration d'instance de région Amazon EC2. Il s'agit d'un modèle de section des paramètres utilisés comme valeurs par défaut lorsque vous ajoutez les configurations d'instance de région Amazon EC2 réelles à partir de l'étape 6.

Pour obtenir une description de chaque paramètre de configuration, voir tableau 31, à la page 244.

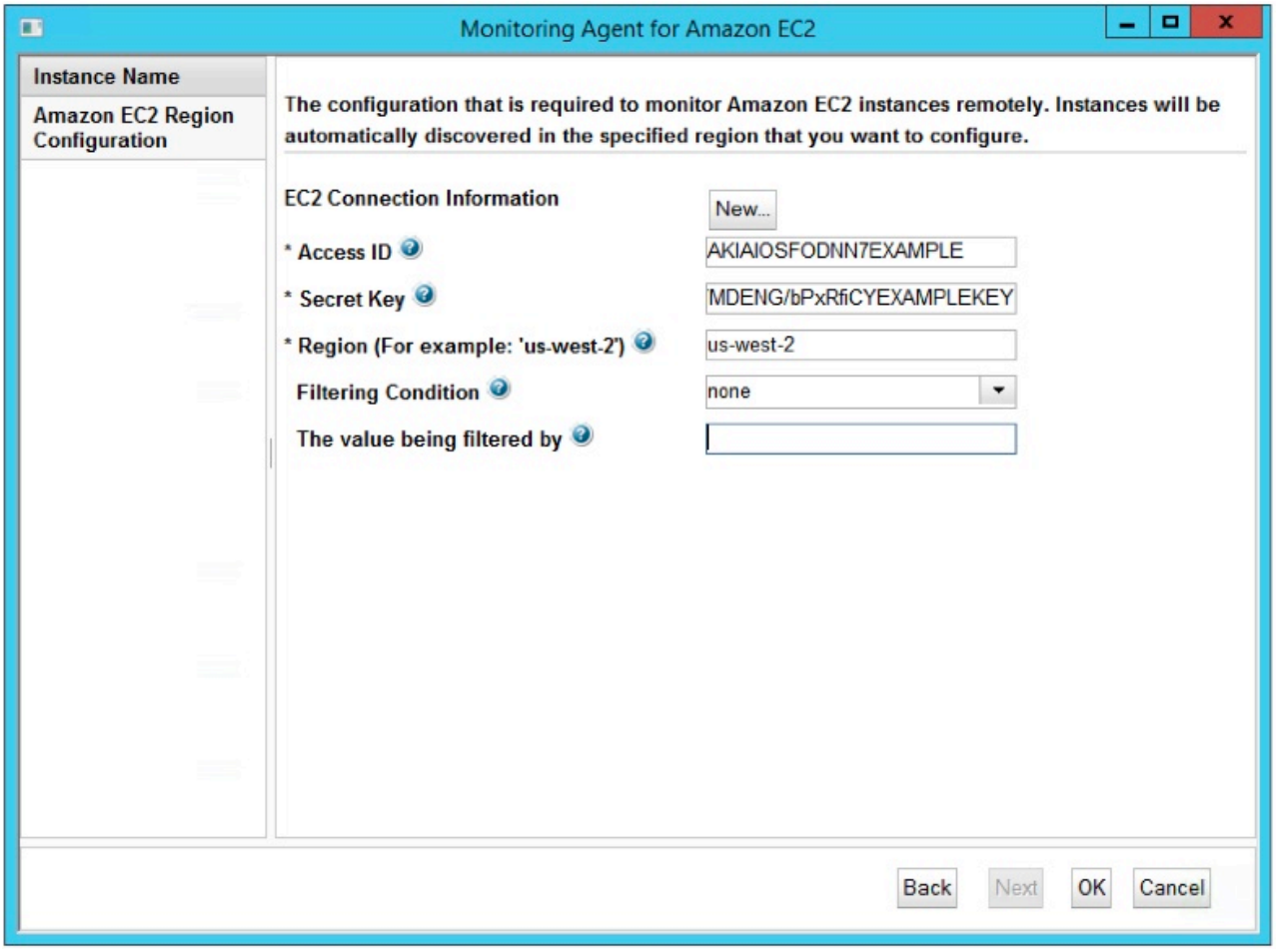


Figure 5. Fenêtre de spécification des paramètres du modèle d'instance de région Amazon EC2.

6. Cliquez sur **Nouveau** et entrez les paramètres d'instance de région Amazon EC2, puis cliquez sur **Suivant**. Voir tableau 31, à la page 244 pour obtenir une description de chaque paramètre de configuration.

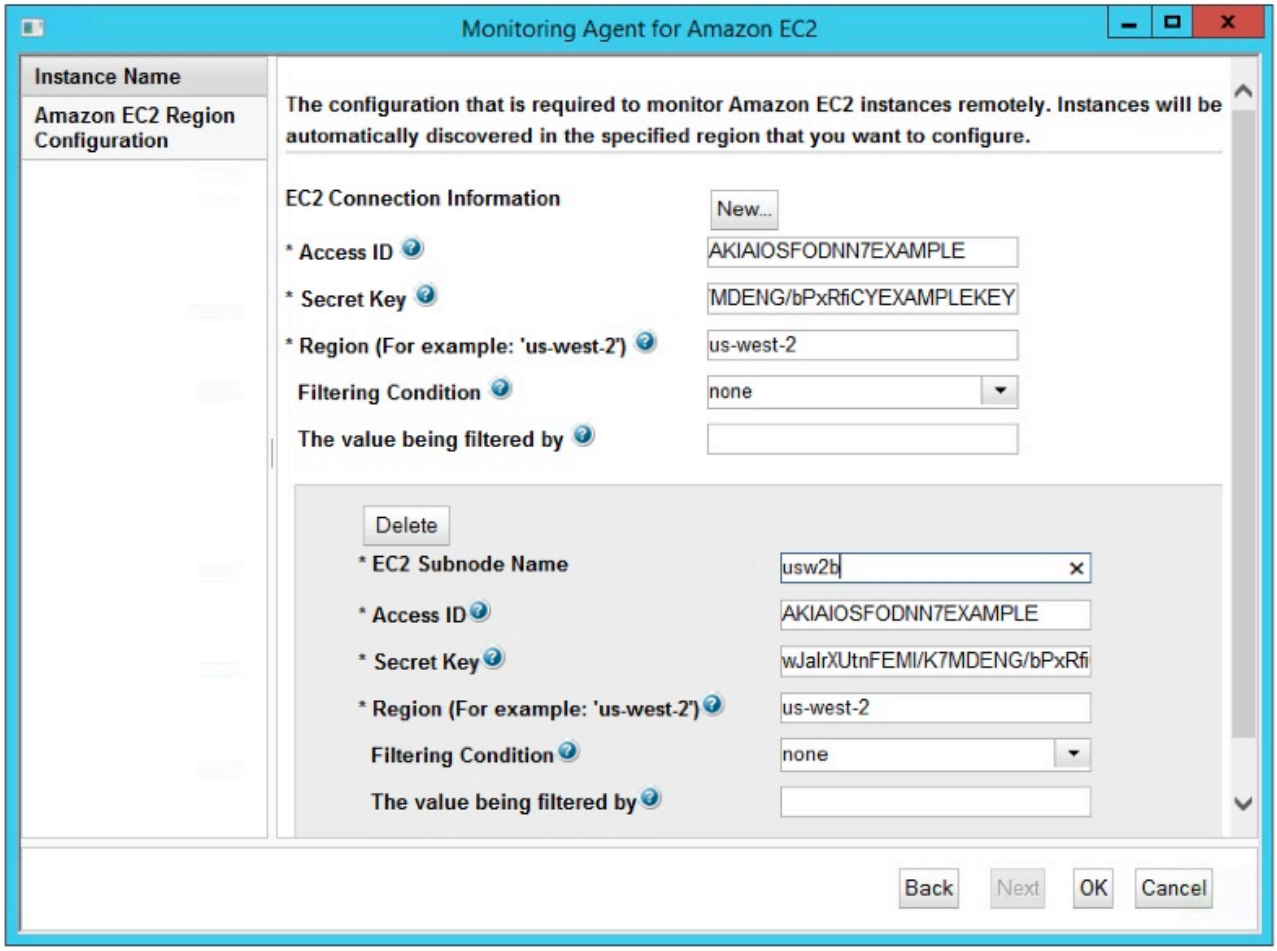


Figure 6. Fenêtre de spécification des paramètres d'instance de région Amazon EC2.

7. Cliquez sur **OK** pour terminer la configuration.
8. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites.

Après avoir installé l'agent Amazon EC2, vous devez le configurer pour pouvoir le démarrer. Si l'agent Amazon EC2 est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Amazon EC2 en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   ```
   rép_install/bin/amazonec2-agent.sh config nom_instance
   ```

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent. Exemple

```
/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3
```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Amazon EC2», à la page 244.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/amazonec2-agent.sh start nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3
   ```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Configurez l'agent Amazon EC2 en mode silencieux :

1. Ouvrez le fichier `amazonec2_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
   - Linux *rép_install*`/samples/amazonec2_silent_config.txt`

     Par exemple, `/opt/ibm/apm/agent/samples/amazonec2_silent_config.txt`
   - Windows *rép_install*`\samples\amazonec2_silent_config.txt`

     Par exemple, `C:\IBM\APM\samples\amazonec2_silent_config.txt`

   où *rép_install* représente le chemin d'installation de l'agent.
2. Dans le fichier `amazonec2_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Voir «Paramètres de configuration de l'agent Amazon EC2», à la page 244 pour obtenir une description de chaque paramètre de configuration.
3. Sauvegardez et fermez le fichier `amazonec2_silent_config.txt`, puis exécutez la commande suivante :
   - Linux *rép_install*`/bin/amazonec2-agent.sh config` **nom_instance** *rép_install*`/samples/amazonec2_silent_config.txt`

     Par exemple, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3 /opt/ibm/apm/agent/samples/amazonec2_silent_config.txt**
   - Windows *rép_install*`\bin\amazonec2-agent.bat config` **nom_instance** *rép_install*`\samples\amazonec2_silent_config.txt`

     Par exemple, **C:\IBM\APM\bin\amazonec2-agent.bat config ec2-inst3 C:\IBM\APM\samples\amazonec2_silent_config.txt**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*/bin/amazonec2-agent.sh start **nom_instance**
     Par exemple, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3**
   - Windows *rép_install*\bin\amazonec2-agent.bat start **nom_instance**
     Par exemple, **C:\IBM\APM\bin\amazonec2-agent.bat start ec2-inst3**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Paramètres de configuration de l'agent Amazon EC2

Les paramètres de configuration de l'agent Amazon EC2 sont regroupés dans un tableau.

1. Configuration des régions Amazon EC2 : paramètres utilisés pour la surveillance à distance des instances Amazon EC2. Les instances sont automatiquement découvertes dans la région spécifiée que vous voulez configurer.

Tableau 31. Configuration des régions Amazon EC2

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du sous-noeud EC2	Nom du sous-noeud EC2 utilisé pour la collecte de données. Par exemple, *usw2a*. Cet alias fait partie du nom de système géré (MSN) et permet d'identifier visuellement l'environnement surveillé dans la console Cloud APM. **Remarque :** Cet alias représente l'instance du sous-noeud Amazon EC2 avec les restrictions suivantes. Vous pouvez utiliser des lettres de l'alphabet latin (a-z, A-Z), des chiffres arabes (0-9), le trait d'union/signe moins (-) et le caractère de soulignement (_) pour créer des noms d'instances de sous-noeud d'agent. La longueur maximale d'un nom de sous-noeud EC2 est de 25 caractères.	Chacun des paramètres suivants doit avoir un suffixe de nom de sous-noeud d'agent qui sera le même pour chaque paramètre d'une instance de sous-noeud d'agent. Les nouvelles instances de sous-noeud d'agent doivent utiliser un nom unique pour son ensemble de paramètres. Par exemple, une instance de sous-noeud d'agent peut utiliser *.usw2a*, tandis qu'une autre peut utiliser *.usw2b* en lieu et place de *.nom_sous_noeud* dans les noms de paramètres qui suivent.
ID d'accès	ID de clé d'accès des droits de sécurité AWS servant à l'authentification auprès de la région Amazon spécifiée. Par exemple, 'AKIAxxxxxxxxxxxxxx'.	**KB5_INS_ACCESS_ID.nom_sous_noeud**
Clé secrète	Clé d'accès secrète des droits de sécurité AWS servant à l'authentification auprès de la région Amazon spécifiée. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.	**KB5_INS_SECRET_KEY.nom_sous_noeud**
Région	Région AWS à surveiller. Par exemple, 'us-west-2'.	**KB5_INS_REGION.nom_sous_noeud**

Tableau 31. Configuration des régions Amazon EC2 (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Condition de filtrage	Type de filtrage effectué. Vous pouvez utiliser des balises personnalisées sur les instances EC2 afin de limiter les instances EC2 qui sont surveillées par l'agent. Pour plus d'informations, voir Tagging Your Amazon EC2 Resources. Options de filtrage : **none** Toutes les instances EC2 au sein de la région sont surveillées. Le paramètre **`Valeur de filtre`** est ignoré. **tagName** Les instances EC2 possédant la clé de balise indiquée dans **`Valeur de filtre`** sont surveillées, quelle que soit la valeur réelle spécifiée dans la valeur de balise d'instance EC2 correspondante. Par exemple, pour surveiller toutes les instances EC2 possédant la clé de balise *Stack*, quelle que soit la valeur spécifiée dans sa valeur de balise, indiquez `Stack` dans **`Valeur de filtre`**. **tagName|tagValue** Les instances EC2 possédant la clé de balise et la paire de valeurs de balises qui est séparée par une barre verticale (`|`) et indiquée dans **`Valeur de filtre`** sont surveillées. Par exemple, pour surveiller toutes les instances EC2 possédant la clé de balise *Stack* et la valeur de balise *Production*, indiquez `Stack|Production` dans **`Valeur de filtre`**. **monitoring-tag** Les instances EC2 possédant au moins une balise sont surveillées. Le paramètre **`Valeur de filtre`** est ignoré.	**`FILTER_CONDITION.nom_sous_noeud`** Les valeurs possibles sont les suivantes : **none** néant **tagName** tagName **tagName|tagValue** tagName|tagValue **monitoring-tag** monitoring-tag
Valeur de filtre	Valeur de la balise selon laquelle les instances EC2 sont filtrées lorsque `tagName` ou `tagName|tagValue` sont sélectionnés pour **`Condition de filtrage`**.	**`FILTER_VALUE.nom_sous_noeud`**

Configuration de la surveillance d'AWS Elastic Load Balancer

L'agent Amazon ELB permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos équilibreurs de charge élastiques AWS. L'agent affiche un ensemble complet de mesures pour chaque type d'équilibreur de charge, application, réseau et classique, qui vous aident à prendre des décisions avisées concernant votre environnement AWS Elastic Load Balancer.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance d'AWS Elastic Load Balancer», à la page 245 pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, voir tableau 32.

Tableau 32. Versions d'agent

Version d'agent	Documentation
1.0.0.0, 1.0.0.1	Cloud APM 8.1.4

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Amazon ELB. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Amazon ELB.
- Vérifiez que les informations suivantes sont disponibles :
  - Les droits de sécurité AWS (ID de clé d'accès et clé d'accès secrète) avec l'autorisation d'accès à chaque région AWS avec les équilibreurs de charge élastiques.

Pourquoi et quand exécuter cette tâche

L'agent Amazon ELB est à la fois un agent à plusieurs instances et un agent de sous-noeud. Les sous-noeuds sont créés automatiquement pour chaque type d'équilibreur de charge élastique disponible dans votre environnement AWS.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows».
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 249.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant aux invites», à la page 248.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 249.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Amazon ELB sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for AWS Elastic Load Balancer**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `elb-inst3`. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 205.

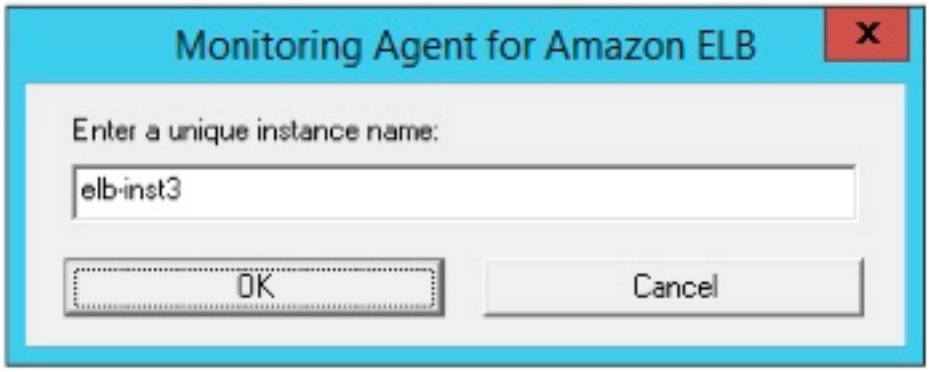


Figure 7. Fenêtre de saisie d'un nom d'instance d'agent unique.

4. Entrez les **données d'identification d'abonnement Amazon ELB**, puis cliquez sur **Suivant**. Voir «Paramètres de configuration de l'agent Amazon ELB», à la page 251 pour obtenir une description de chaque paramètre de configuration.

   Important : Windows Si votre **clé secrète/mot de passe** contient le signe égal (=), vous devez la/le saisir à nouveau chaque fois que vous reconfigurez l'agent.

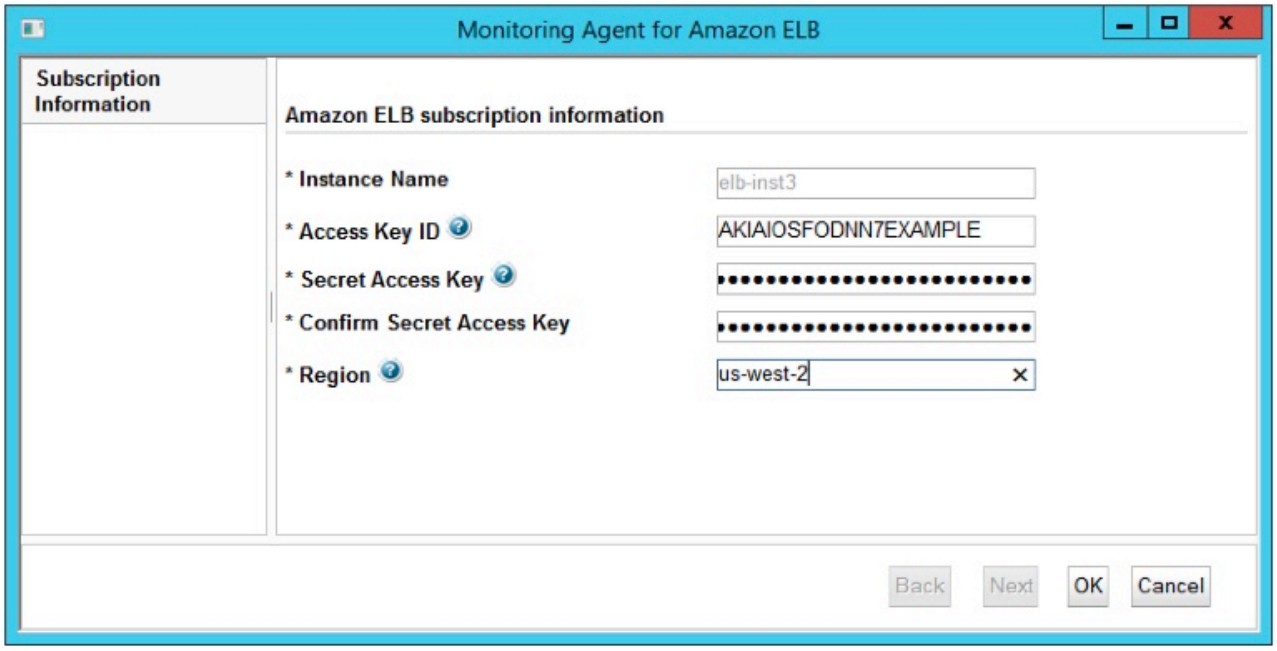


Figure 8. Fenêtre des données d'identification d'abonnement Amazon ELB.

5. Cliquez sur **OK** pour terminer la configuration.
6. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant aux invites

Après avoir installé l'agent Amazon ELB, vous devez le configurer pour pouvoir le démarrer. Si l'agent Amazon ELB est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Amazon ELB en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   rép_install`/bin/amazon_elb-agent.sh config` *nom-instance*

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 205. Exemple

   ```
   /opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Amazon ELB», à la page 251.

3. Exécutez la commande suivante pour démarrer l'agent :

rép_install/bin/amazon_elb-agent.sh start **nom-instance**

Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent. Exemple

```
/opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3
```

Exemple

Création d'une instance d'agent nommée elb-inst3.

```
# ./amazon_elb-agent.sh config elb-inst3
Configuring Monitoring Agent for Amazon ELB

Edit 'Monitoring Agent for Amazon ELB' settings? [1=Yes,2=No](default is: 1): 1

Subscription Information :
Amazon ELB subscription information

The access ID that is used to authenticate with the specified Amazon Region.
Par exemple, 'AKIAxxxxxxxxxxxxxx'.
Access Key ID (default is: ): AKIAIOSFODNN7EXAMPLE

The secret access key that is used to authenticate with the specified Amazon
Region. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxxx'.
Enter Secret Access Key (default is: ): hidden

Re-type : Secret Access Key (default is: ): hidden

The Amazon region where the load balancers are located. Par exemple, 'us-west-2'.
Region (default is: ): us-west-2

Configuration completed successfully.
Automatic start at system initialization has been configured.
Automatic stop at system shutdown has been configured.
```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Procédez comme suit pour configurer l'agent Amazon ELB en mode silencieux.

1. Ouvrez le fichier amazon_elb_silent_config.txt qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
   - Linux *rép_install*/samples/amazon_elb_silent_config.txt
     Par exemple, /opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt
   - Windows *rép_install*\samples\amazon_elb_silent_config.txt
     Par exemple, C:\IBM\APM\samples\amazon_elb_silent_config.txt

Où *rép_install* représente le chemin d'installation de l'agent.

2. Dans le fichier `amazon_elb_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Voir «Paramètres de configuration de l'agent Amazon ELB», à la page 251 pour obtenir une description de chaque paramètre de configuration.

3. Sauvegardez et fermez le fichier `amazon_elb_silent_config.txt`, puis exécutez la commande suivante :

   - Linux *rép_install*`/bin/amazon_elb-agent.sh config` **nom-instance** *rép_install*`/samples/amazon_elb_silent_config.txt`

     Par exemple, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3 /opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt**

   - Windows *rép_install*`\bin\amazon_elb-agent.bat config` **nom-instance** *rép_install*`\samples\amazon_elb_silent_config.txt`

     Par exemple, **C:\IBM\APM\bin\amazon_elb-agent.bat config elb-inst3 C:\IBM\APM\samples\amazon_elb_silent_config.txt**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 205.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Exécutez la commande suivante pour démarrer l'agent :

   - Linux *rép_install*`/bin/amazon_elb-agent.sh start` **nom-instance**

     Par exemple, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3**

   - Windows *rép_install*`\bin\amazon_elb-agent.bat start` **nom-instance**

     Par exemple, **C:\IBM\APM\bin\amazon_elb-agent.bat start elb-inst3**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent.

Exemple

Fichier `amazon_elb_silent_config.txt` édité.

```
#
# Ce fichier est un exemple de fichier de réponses de configuration pour l'agent Amazon ELB.
#
# Il contient une entrée pour chaque propriété de configuration.
# Les entrées des propriétés facultatives qui n'ont pas de valeur par défaut sont incluses
# dans les commentaires.
# Vérifiez que toutes les propriétés non mises en commentaires ont une valeur avant de configurer
# l'agent.
#

# ID de clé d'accès : ID d'accès servant à l'authentification auprès
# de la région Amazon spécifiée. Par exemple, 'AKIAxxxxxxxxxxxxxx'.
KAL_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

# Clé d'accès secrète : clé d'accès secrète servant à l'authentification auprès
# de la région Amazon spécifiée. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxxxx'.
KAL_SECRET_ACCESS_KEY_PASSWORD=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

# Région : région Amazon où se trouvent les équilibreurs de charge. Par
# exemple, 'us-west-2'.
KAL_REGION=us-west-2
```

Paramètres de configuration de l'agent Amazon ELB

Les paramètres de configuration de l'agent Amazon ELB sont regroupés dans un tableau.

1. tableau 33 - Données d'identification requises pour accéder à l'abonnement Amazon qui contient les équilibreurs de charge élastiques AWS à surveiller.

Tableau 33. Informations sur l'abonnement

Nom de paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
ID clé d'accès	ID d'accès servant à l'authentification auprès de la région Amazon spécifiée. Par exemple, 'AKIAxxxxxxxxxxxxxx'.	**KAL_ACCESS_KEY_ID**
Clé d'accès secrète	Clé d'accès secrète servant à l'authentification auprès de la région Amazon spécifiée. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxxx'.	**KAL_SECRET_ACCESS_KEY_PASSWORD**
Région	Région Amazon où se trouvent les équilibreurs de charge. Par exemple, 'us-west-2'.	**KAL_REGION**

Configuration de la surveillance Azure Compute

L'Agent Azure Compute permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Azure Compute. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement Azure Compute. Ces mesures incluent l'utilisation de l'UC, l'utilisation du réseau et les performances du disque.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance Azure Compute» pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, voir tableau 34.

Tableau 34. Versions d'agent

Version d'agent	Documentation
1.0.0.0	Cloud APM 8.1.4

- Assurez-vous que votre environnement possède la configuration système requise pour l'Agent Azure Compute. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Azure Compute.
- Vérifiez que les informations suivantes sont disponibles :
  - Les données d'identification d'abonnement Azure avec le droit d'accéder aux instances Azure Compute à surveiller.

Pourquoi et quand exécuter cette tâche

L'Agent Azure Compute est à la fois un agent à plusieurs instances et un agent de sous-noeud. Chaque sous-noeud de l'Agent Azure Compute surveille un regroupement de machines virtuelles Azure Compute en fonction du filtre que vous définissez. Vous pouvez créer une instance d'agent à plusieurs sous-noeuds (un pour chaque regroupement de machines virtuelles) ou une instance d'agent pour chaque regroupement de machines virtuelles avec un sous-noeud pour ce regroupement . Vous pouvez également créer une combinaison de chaque type de configuration. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement. Il est conseillé de ne pas avoir plus de 50 ressources par regroupement de machines virtuelles Azure Compute. Chaque nom de sous-noeud de l'agent Azure

Compute doit être unique dans votre environnement.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows».
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 257.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 255.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 257.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent Azure Compute sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Azure Compute**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `azc-inst3`. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 205.

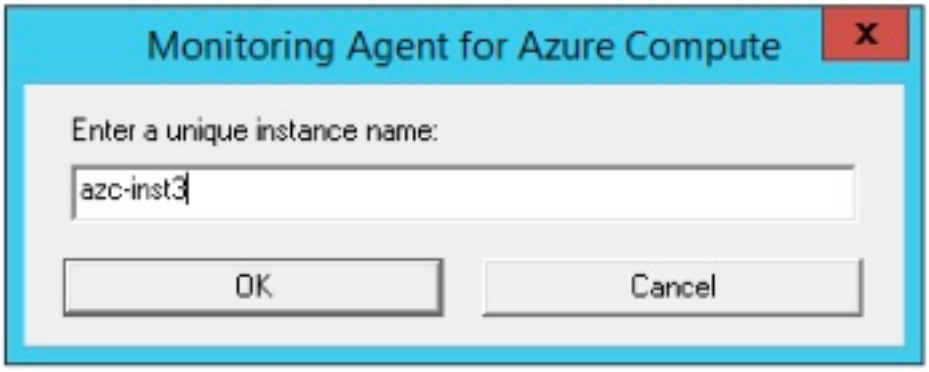


Figure 9. Fenêtre de saisie d'un nom d'instance d'agent unique.

4. Entrez les **données d'identification d'abonnement Azure**, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 35, à la page 259.

   Important : Windows Si votre **clé secrète/mot de passe** contient le signe égal (=), vous devez la/le saisir à nouveau chaque fois que vous reconfigurez l'agent.

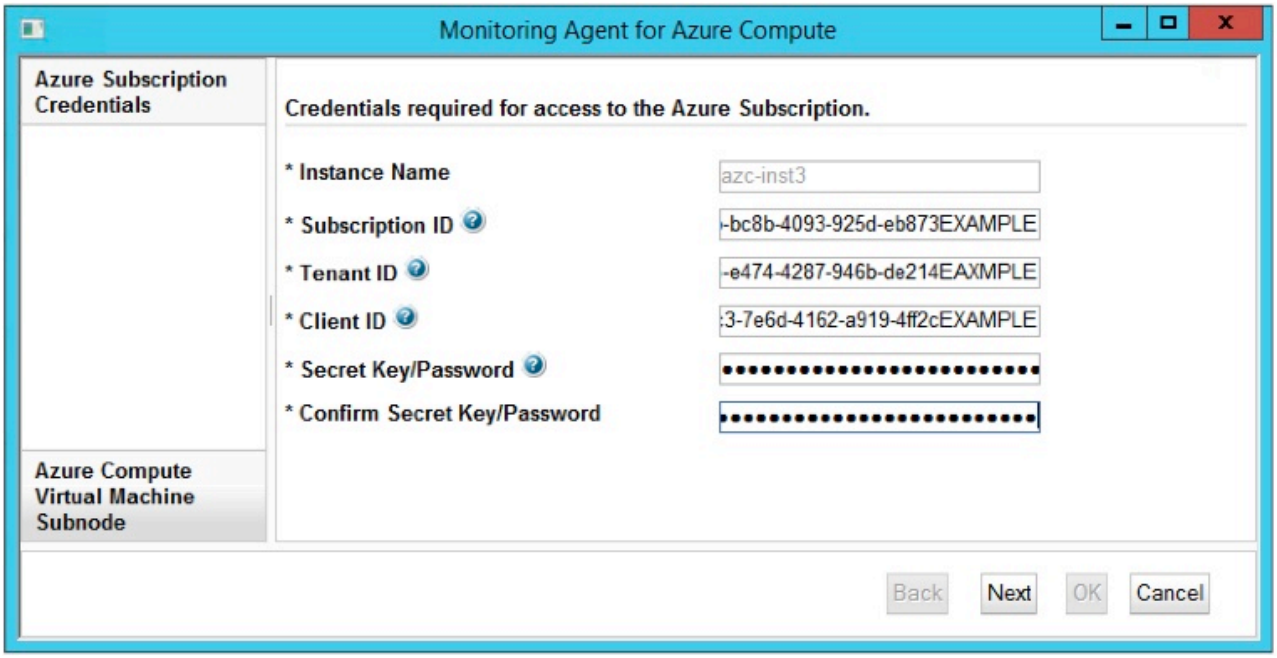


Figure 10. Fenêtre des données d'identification d'abonnement Azure.

5. Entrez les paramètres du modèle de **sous-noeud de machine virtuelle Azure Compute**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 36, à la page 260.

   Remarque : Cette section ne permet pas de configurer l'instance du sous-noeud de machine virtuelle Azure Compute. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut utilisées lorsque vous ajoutez les configurations réelles de l'instance du sous-noeud de machine virtuelle Azure Compute à l'étape 6.

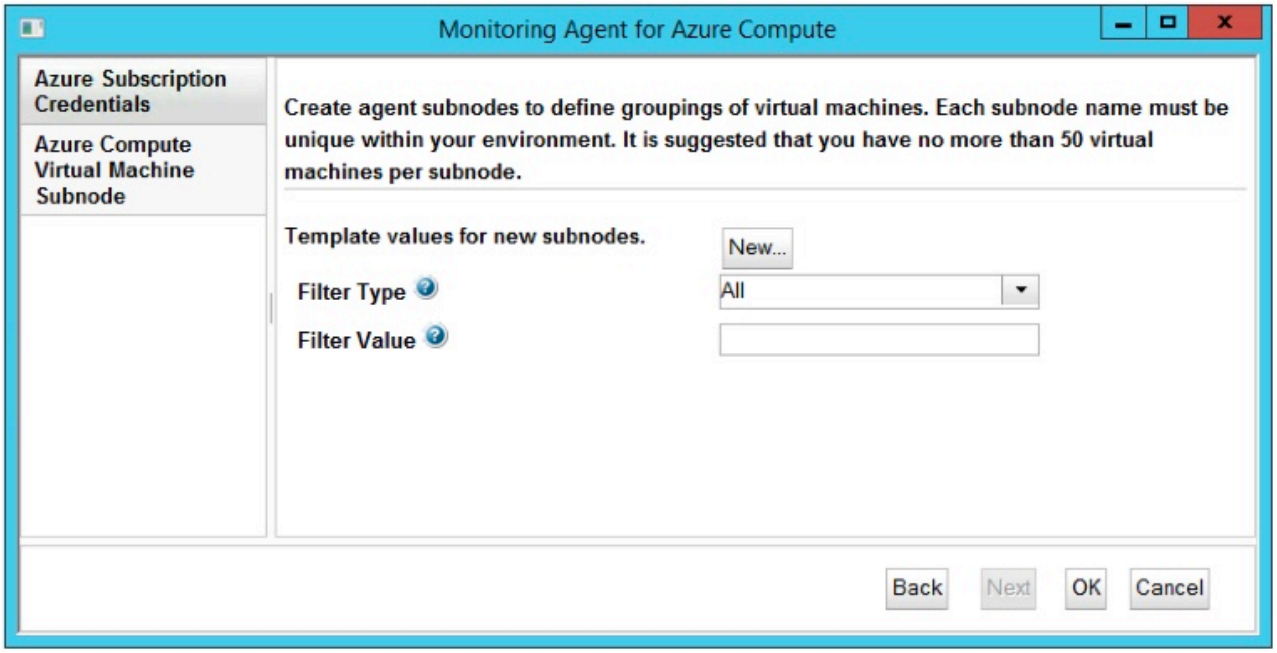


Figure 11. Fenêtre de spécification des paramètres de modèle de sous-noeud de machine virtuelle Azure Compute.

6. Cliquez sur **Nouveau** et entrez les paramètres de l'instance du **sous-noeud de machine virtuelle Azure Compute**, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 36, à la page 260.

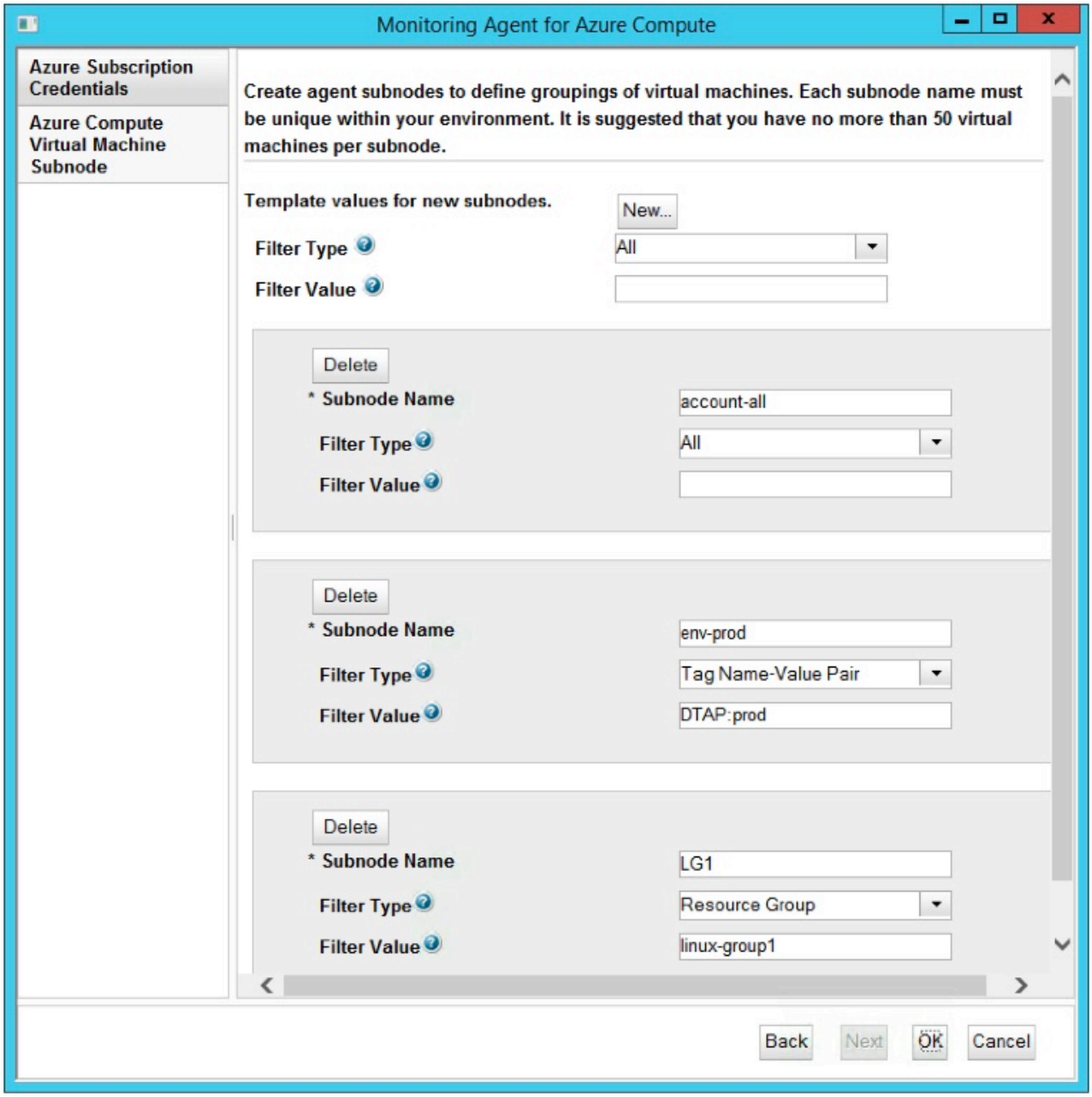


Figure 12. Fenêtre de spécification des paramètres de l'instance du sous-noeud de machine virtuelle Azure Compute.

7. Cliquez sur **OK** pour terminer la configuration.
8. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'Agent Azure Compute, vous devez le configurer pour pouvoir le démarrer. Si l'Agent Azure Compute est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'Agent Azure Compute en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   rép_install/bin/azure_compute-agent.sh config *nom-instance*

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 205. Exemple

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent Azure Compute», à la page 259.

   A faire : Lorsque vous configurez une instance d'agent pour la première fois, vous devez ajouter au moins un sous-noeud lorsque vous êtes invité à modifier les paramètres du sous-noeud de machine virtuelle Azure Compute (**Edit 'Azure Compute Virtual Machine Subnode' settings**).

3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/azure_compute-agent.sh start **nom-instance**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3
   ```

Exemple

Création d'une instance d'agent nommée azc-inst3 et dotée d'une instance de sous-noeud nommée azc1.

```
# ./azure_compute-agent.sh config azc-inst3
Configuring Monitoring Agent for Azure Compute

Edit 'Monitoring Agent for Azure Compute' settings? [1=Yes,2=No](default is: 1): 1

Azure Subscription Credentials :
Credentials required for access to the Azure Subscription.

The ID assigned by Azure for the Subscription that is monitored.
Subscription ID (default is: ): 09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE

The tenant ID that is assigned by Azure. Used to log in to the Azure service API.
Tenant ID (default is: ): 75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE

The client ID that is assigned by Azure to identify this agent as an external
application that monitors the Azure compute services.
Client ID (default is: ): 79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE

The secret access key or password that is created by Azure for the client application.
Enter Secret Key/Password (default is: ): hidden

Re-type : Secret Key/Password (default is: ): hidden

Azure Compute Virtual Machine Subnode :
```

```
Create agent subnodes to define groupings of virtual machines. Each subnode name
must be unique within your environment. It is suggested that you have no more
than 50 virtual machines per subnode.

No 'Azure Compute Virtual Machine Subnode' settings available.
Edit 'Azure Compute Virtual Machine Subnode' settings, [1=Add, 2=Edit, 3=Del,
4=Next, 5=Exit] (default is: 5): 1
Subnode Name (default is: ): azc1
The type of filter to be applied.
Filter Type [ 1=All, 2=Tag Name-Value Pair, 3=Resource Group ] (default is: 1): 2
The filter value corresponding to the selected Filter Type. This value can be a
Resource Group or Tag Name-Value Pair, for example Environment\:Production.
A backslash might appear in the example, do not enter a backslash in the value
you provide.
Filter Value (default is: ): Environment:Production



Azure Compute Virtual Machine Subnode settings: Subnode Name=azc1
Edit 'Azure Compute Virtual Machine Subnode' settings, [1=Add, 2=Edit, 3=Del,
4=Next, 5=Exit] (default is: 5): 5
Configuration completed successfully.
Automatic start at system initialization has been configured.
Automatic stop at system shutdown has been configured.
You have new mail in /var/spool/mail/root
```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Procédez comme suit pour configurer l'Agent Azure Compute en mode silencieux.

1. Ouvrez le fichier `azure_compute_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
   - Linux *rép_install*`/samples/azure_compute_silent_config.txt`
     Par exemple, `/opt/ibm/apm/agent/samples/azure_compute_silent_config.txt`
   - Windows *rép_install*`\samples\azure_compute_silent_config.txt`
     Par exemple, `C:\IBM\APM\samples\azure_compute_silent_config.txt`

   Où *rép_install* représente le chemin d'installation de l'agent.
2. Dans le fichier `azure_compute_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent Azure Compute», à la page 259.

   Important : Vous devez activer et spécifier les paramètres Filter Type et Filter Value pour au moins un nom de sous-noeud.

3. Sauvegardez et fermez le fichier azure_compute_silent_config.txt et exécutez la commande suivante :
   - Linux *rép_install*/bin/azure_compute-agent.sh config **nom-instance** *rép_install*/samples/azure_compute_silent_config.txt

     Par exemple, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3 /opt/ibm/apm/agent/samples/azure_compute_silent_config.txt**
   - Windows *rép_install*\bin\azure_compute-agent.bat config **nom-instance** *rép_install*\samples\azure_compute_silent_config.txt

     Par exemple, **C:\IBM\APM\bin\azure_compute-agent.bat config azc-inst3 C:\IBM\APM\samples\azure_compute_silent_config.txt**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 205.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*/bin/azure_compute-agent.sh start **nom-instance**

     Par exemple, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3**
   - Windows *rép_install*\bin\azure_compute-agent.bat start **nom-instance**

     Par exemple, **C:\IBM\APM\bin\azure_compute-agent.bat start azc-inst3**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent.

Exemple

Fichier azure_compute_silent_config.txt édité avec trois sous-noeuds nommés account-all, env-prod et LG1.

```
#
# Ce fichier est un exemple de fichier de réponses de configuration pour l'agent Azure Compute.
#
# Il contient une entrée pour chaque propriété de configuration.
# Les entrées des propriétés facultatives qui n'ont pas de valeur par défaut sont incluses
# dans les commentaires.
# Les entrées du sous-noeud AVM se voient attribuer l'exemple de nom d'instance de sous-noeud avm1.
# Vérifiez que toutes les propriétés non mises en commentaires ont une valeur avant de configurer
# l'agent.
#

# ID abonnement : ID attribué par Azure à l'abonnement
# surveillé.
KAK_SUBSCRIPTION_ID=09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE
# ID titulaire : ID titulaire attribué par Azure. Permet de se connecter à
# l'API du service Azure.
KAK_TENANT_ID=75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE
# ID client : ID client attribué par Azure pour identifier cet agent
# en tant qu'application externe
# qui surveille les services Azure Compute.
KAK_CLIENT_ID=79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE
# Clé secrète/Mot de passe : clé d'accès secrète ou mot de passe créé(e) par
# Azure pour l'application client.
KAK_SECRET_PASSWORD=hZxWPq/IOxlnvg/wdxLwTf2Fs3x2sWQV/sCE-EXAMPLE

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
#KAK_FILTER_TYPE.avm1=ALL
```

```
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
#KAK_FILTER_VALUE.avm1=

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
KAK_FILTER_TYPE.account-all=ALL
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
KAK_FILTER_VALUE.account-all=

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
KAK_FILTER_TYPE.env-prod=TAG_NAME_VALUE
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
KAK_FILTER_VALUE.env-prod=DTAP:prod

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
KAK_FILTER_TYPE.LG1=RESOURCE_GROUP
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
KAK_FILTER_VALUE.LG1=linux-group1
```

Paramètres de configuration de l'Agent Azure Compute

Les paramètres de configuration de l'Agent Azure Compute sont affichés dans des tableaux qui les regroupent par sections.

1. tableau 35 - Données d'identification requises pour accéder à l'abonnement Azure qui contient les ressources Azure Compute à surveiller.
2. tableau 36, à la page 260 - Créez des sous-noeuds d'agent pour définir des regroupements de machines virtuelles. Chaque nom du sous-noeud doit être unique dans votre environnement. Il est conseillé de ne pas avoir plus de 50 machines virtuelles par sous-noeud.

Tableau 35. Données d'identification pour l'abonnement Azure

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
ID abonnement	ID attribué par Azure pour l'abonnement surveillé.	**KAK_SUBSCRIPTION_ID**
ID titulaire	ID titulaire attribué par Azure. Permet de se connecter à l'API de service Azure.	**KAK_TENANT_ID**
ID client	ID client affecté par Azure pour identifier cet agent en tant qu'application externe qui surveille les services Azure Compute.	**KAK_CLIENT_ID**

Tableau 35. Données d'identification pour l'abonnement Azure (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Clé secrète/Mot de passe	Clé d'accès secrète ou mot de passe créé(e) par Azure pour l'application client. **Important :** Windows Si votre **clé secrète/mot de passe** contient le signe égal (=), vous devez la/le saisir à nouveau chaque fois que vous reconfigurez l'agent.	**KAK_SECRET_PASSWORD**

Tableau 36. Sous-noeud de machine virtuelle Azure Compute

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du sous-noeud	Nom du sous-noeud Azure Compute utilisé pour la collecte de données. Par exemple, *azc1*. Le nom du sous-noeud doit être unique dans votre environnement. Cet alias fait partie du nom de système géré (MSN) et permet d'identifier visuellement l'environnement surveillé dans la console Cloud APM. **Remarque :** Cet alias représente l'instance du sous-noeud Azure Compute avec les restrictions suivantes. Vous pouvez utiliser des lettres de l'alphabet latin (a-z, A-Z), des chiffres arabes (0-9), le trait d'union/signe moins (-) et le caractère de soulignement (_) pour créer des noms d'instances de sous-noeud d'agent. La longueur maximale d'un nom de sous-noeud Azure Compute est de 25 caractères.	Chacun des paramètres suivants doit contenir un point (.) suivi du **nom de sous-noeud** d'agent comme suffixe. Le **nom du sous-noeud** doit être identique pour chaque paramètre de sous-noeud. Les nouvelles instances de sous-noeud d'agent doivent utiliser un **nom de sous-noeud** unique pour son ensemble de paramètres. Par exemple, une instance de sous-noeud d'agent peut utiliser *.azc1*, tandis qu'une autre peut utiliser *.azc2* en lieu et place de *.nom_sous_noeud* dans les noms de paramètres qui suivent.
Type de filtre	Type de filtre à appliquer.	**KAK_FILTER_TYPE.nom_sousnoeud** Les valeurs possibles sont les suivantes : **ALL** Tous **TAG_NAME_VALUE** Paire Nom-valeur de balise **RESOURCE_GROUP** Groupe de ressources

Tableau 36. Sous-noeud de machine virtuelle Azure Compute (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Valeur de filtre	Valeur de filtre correspondant au **type de filtre** sélectionné. Cette valeur peut être un **Groupe de ressources** ou une **paire Nom-valeur de balise**. Ne la renseignez pas si le **type de filtre** est défini sur **All**. Pour la configuration sur ligne de commande, une barre oblique inversée peut apparaître dans l'exemple affiché. Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez. Exemples de paires type de filtre/valeur de filtre : • Le sous-noeud Azure Compute surveille toutes les machines virtuelles. Ne renseignez pas la valeur de filtre. Elle n'est pas nécessaire et est ignorée pour le type de filtre **All**. – Type de filtre : **All** – Valeur de filtre : • Le sous-noeud Azure Compute surveille toutes les machines virtuelles dont le nom de balise est `DTAP` et dotées d'une valeur de balise correspondant à la chaîne `prod`. – Type de filtre : **Paire Nom-valeur de balise** – Valeur de filtre : `DTAP:prod` • Le sous-noeud Azure Compute surveille toutes les machines virtuelles dotées d'une propriété Groupe de ressources correspondant à la chaîne `linux-group1`. – Type de filtre : **Groupe de ressources** – Valeur de filtre : `linux-group1`	**KAK_FILTER_VALUE.nom_sousnoeud**

Configuration de la surveillance de Cassandra

Vous devez configurer l'agent Cassandra pour qu'il puisse collecter les données issues des noeuds au sein du cluster afin de surveiller l'état de santé de la base de données Cassandra.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for Cassandra agent

Pourquoi et quand exécuter cette tâche

L'agent Cassandra est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation de la version 1.0, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Pour pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**. La fenêtre Agent de surveillance pour Cassandra s'ouvre.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre Agent de surveillance pour Cassandra, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 264.
5. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur les systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance : `./cassandra-agent.sh config nom_instance`
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 et entrez :

   ```
   Edit 'Monitoring Agent for Cassandra' setting? [1=Yes, 2=No]
   ```
4. A l'invite, indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 264.
5. Exécutez la commande suivante pour démarrer l'agent :

   ```
   ./cassandra-agent.sh start nom_instance
   ```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent Cassandra sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de configuration en mode silencieux qui est disponible à l'emplacement suivant et indiquez des valeurs pour tous les paramètres : Windows *rép_install*\samples\cassandra_silent_config_windows.txt
   Linux *rép_install*\samples\cassandra_silent_config_UNIX.txt
   Windows C:\IBM\APM\samples
   Linux /opt/ibm/apm/agent/samples
   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 264.
2. Sur la ligne de commande, changez le chemin d'accès au *rép_install* \casier.
3. Exécutez la commande suivante :
   Windows cassandra-agent.bat config *nom_instance rép_install*\samples\cassandra_silent_config_windows.txt
   Linux cassandra-agent.sh config *nom_instance rép_install*\samples\cassandra_silent_config_UNIX.txt
4. Démarrez l'agent.
   Windows Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.
   Linux Exécutez la commande suivante : ./cassandra-agent.sh start *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'agent Cassandra, vous pouvez modifier la valeur par défaut des paramètres, comme Adresse IP et JMX_PORT.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'agent Cassandra.

Tableau 37. Noms et descriptions des paramètres de configuration

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	La valeur par défaut de cette zone est identique à celle que vous indiquez dans la zone **Enter a unique instance name**.	Oui
Adresse IP	Adresse IP de n'importe quel noeud dans le cluster.	Oui
JMX_PORT	Numéro de port JMX permettant d'activer la surveillance. **Important :** Veillez à spécifier le Port JMX, le Nom d'utilisateur JMX et le mot de passe JMX dans l'ensemble du cluster. Si le noeud qui connecte l'agent au cluster ne fonctionne pas, l'agent peut collecter des données par le biais d'un autre noeud dans le cluster en utilisant les mêmes paramètres.	Oui
JMX_Username	Nom d'utilisateur permettant d'accéder à JMX.	Non
JMX_Password	Mot de passe permettant d'accéder à JMX.	Non

Configuration de la surveillance de Cisco UCS

L'Monitoring Agent for Cisco UCS surveille l'infrastructure virtuelle Cisco UCS en se connectant à Cisco UCSM. Vous devez configurer l'agent Cisco UCS de sorte qu'il puisse collecter les données Cisco UCS.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Cisco UCS.
- Vérifiez que l'utilisateur, qui se connecte à l'infrastructure Cisco UCS, dispose des privilèges aaa ou d'administrateur. Utilisez un utilisateur existant disposant des privilèges aaa ou d'administrateur, ou créez un nouvel ID utilisateur.
- Si l'agent Cisco UCS est configuré pour communiquer avec ses sources de données Cisco UCS qui utilisent l'agent SSL, ajoutez le certificat SSL de chaque source de données au magasin de clés de confiance de certificats de l'agent. Pour plus d'informations sur l'activation de la communication SSL avec les sources de données Cisco UCS, voir «Activation de la communication SSL avec les sources de données Cisco UCS», à la page 269.

Pourquoi et quand exécuter cette tâche

L'agent Cisco UCS est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 38. Versions d'agent et documentation

Version de l'agent Cisco UCS	Documentation
7.2.0.4, 7.2.0.3	IBM Cloud Application Performance Management

Tableau 38. Versions d'agent et documentation (suite)

Version de l'agent Cisco UCS	Documentation
7.2.0.2	IBM Performance Management 8.1.3 *
7.2.0.1	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Les attributs de configuration définissent l'infrastructure Cisco UCS qui est surveillée. Les attributs définissent une connexion à Cisco UCSM 1.4 ou ultérieure. Vous pouvez configurer plusieurs instances de l'agent de surveillance sur un système hôte de surveillance distant. Vous pouvez également créer des instances distinctes pour surveiller une infrastructure Cisco UCS spécifique.

Une fois l'agent Cisco UCS installé, vous pouvez le démarrer. Vous devez cependant le configurer manuellement pour afficher les données de tous les attributs d'agent.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'agent Cisco UCS fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Cisco UCS**, puis sur **Configuration de l'agent**.

   A faire : Après avoir configuré l'agent pour la première fois, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Monitoring Agent for Cisco UCS, procédez comme suit :
   a. Entrez un nom unique pour l'instance d'agent Cisco UCS et cliquez sur **OK**.
   b. Dans l'onglet **CONFIG**, spécifiez les valeurs des paramètres de configuration et cliquez sur **Suivant**.
   c. Dans l'onglet **LOG_CONFIG**, spécifiez les valeurs des paramètres de configuration et cliquez sur **Suivant**.

   Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Monitoring Agent for Cisco UCS, consultez les rubriques suivantes :
   - «Paramètres de configuration pour l'agent», à la page 268
   - «Paramètres de configuration pour le fournisseur de données», à la page 268
4. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Cisco UCS**, puis sur **Démarrer**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java™. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 270.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent Cisco UCS en mode silencieux, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier `cisco_ucs_silent_config.txt` disponible à l'emplacement suivant :
   - Linux *rép_install*`/samples/cisco_ucs_silent_config.txt`

     Exemple : `/opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`
   - Windows *rép_install*`\samples\cisco_ucs_silent_config.txt`

     Exemple : `C:\IBM\APM\samples\cisco_ucs_silent_config.txt`
2. Dans le fichier `cisco_ucs_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
   - «Paramètres de configuration pour l'agent», à la page 268
   - «Paramètres de configuration pour le fournisseur de données», à la page 268
3. Sauvegardez et fermez le fichier `cisco_ucs_silent_config.txt` et exécutez la commande suivante :
   - Linux *rép_install*`/bin/cisco_ucs-agent.sh config` *nom_instance rép_install*`/samples/cisco_ucs_silent_config.txt`

     Exemple : **`/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config nom_instance /opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`**
   - Windows *rép_install*`\bin\cisco_ucs-agent.bat config` *nom_instance rép_install*`\samples\cisco_ucs_silent_config.txt`

     Exemple : **`C:\IBM\APM\bin\cisco_ucs-agent.bat config nom_instance C:\IBM\APM\samples\cisco_ucs_silent_config.txt`**

     Où

nom_instance
Nom à attribuer à l'instance.

rép_install
Chemin d'installation de l'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*/bin/cisco_ucs-agent.sh start *nom_instance*
     Exemple : **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start nom_instance**
   - Windows *rép_install*\bin\cisco_ucs-agent.bat start *nom_instance*
     Exemple : **C:\IBM\APM\bin\cisco_ucs-agent.bat start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java™. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 270.

Configuration de l'agent en répondant aux invites

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Sur la ligne de commande, entrez la commande suivante :
   rép_install/bin/cisco_ucs-agent.sh config *nom_instance*
   Exemple : **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config nom_instance**
   Où

   nom_instance
   Nom à attribuer à l'instance.

   rép_install
   Chemin d'installation de l'agent.
2. Répondez aux invites en vous référant aux rubriques suivantes :
   - «Paramètres de configuration pour l'agent», à la page 268
   - «Paramètres de configuration pour le fournisseur de données», à la page 268
3. Exécutez la commande suivante pour démarrer l'agent :
   rép_install/bin/cisco_ucs-agent.sh start *nom_instance*
   Exemple : **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

- Si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java™. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 270.

Paramètres de configuration pour l'agent

Lorsque vous configurez l'agent Cisco UCS, vous pouvez modifier les valeurs par défaut des paramètres, comme le nom de l'instance et les certificats de validation SSL.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'agent Cisco UCS.

Tableau 39. Noms et descriptions des paramètres de configuration pour l'agent Cisco UCS

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	Nom de l'instance. **Restriction :** La zone **Nom d'instance** contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.	Oui
URL	Adresse URL du gestionnaire Cisco UCS. Pour définir l'adresse URL du gestionnaire Cisco UCS, entrez l'URL au format http://adresse_ip/nuova.	Oui
Nom d'utilisateur	Nom d'utilisateur administrateur du gestionnaire Cisco UCS.	Oui
Mot de passe	Mot de passe administrateur du gestionnaire Cisco UCS.	Oui
Confirmer le mot de passe	Mot de passe que vous avez entré dans la zone **Password**.	Oui
SSL truststore filepath	Chemin d'accès au fichier de clés certifiées SSL. Pour que l'agent valide les certificats SSL lors de l'utilisation de SSL pour communiquer à travers le réseau, spécifiez l'emplacement du fichier de clés certifiées SSL.	Oui
Valider les certificats SSL	Valeur booléenne qui indique si l'agent valide les certificats SSL lorsque l'agent utilise SSL pour communiquer à travers le réseau. Définissez la valeur sur `Yes` pour que l'agent valide les certificats SSL lorsqu'il utilise SSL pour communiquer à travers le réseau. Définissez la valeur sur `No` pour empêcher l'agent de valider les certificats SSL. **Conseil :** Pour plus d'informations sur l'activation de la communication SSL avec les sources de données Cisco UCS, voir «Activation de la communication SSL avec les sources de données Cisco UCS», à la page 269.	Oui

Paramètres de configuration pour le fournisseur de données

Lorsque vous configurez l'agent Cisco UCS, vous pouvez modifier les valeurs par défaut des paramètres pour le fournisseur de données, comme le nombre maximal de fichiers journaux du fournisseur de données, la taille maximale du fichier journal et le niveau de détail inclus dans le fichier journal.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du fournisseur de données.

Tableau 40. Noms et descriptions des paramètres de configuration pour le fournisseur de données

Nom du paramètre	Description	Zone obligatoire
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Taille maximale (en ko) de chaque journal de fournisseur de données	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Niveau de détail dans le journal du fournisseur de données	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est INFO. Les valeurs admises sont les suivantes : OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST et ALL.	Oui

Activation de la communication SSL avec les sources de données Cisco UCS

L'agent Cisco UCS peut être configuré pour communiquer de manière sécurisée avec ses sources de données Cisco UCS via SSL. Dans cette configuration, vous devez ajouter un certificat SSL de source de données dans le magasin de clés de confiance de l'agent.

Pourquoi et quand exécuter cette tâche

Important : Les informations ci-dessous ne s'appliquent que si l'agent est configuré de manière à valider les certificats SSL.

Si la validation de certificat SSL est désactivée, l'agent Cisco UCS se connecte aux sources de données Cisco UCS même si leurs certificats SSL ont expiré, ne sont pas dignes de confiance ou ne sont pas valides. Cependant, la désactivation de la validation des certificats SSL peut poser des problèmes de sécurité et doit être effectuée avec précaution.

Si une source de données Cisco UCS utilise un certificat SSL signé par une autorité de certification commune (par exemple Verisign, Entrust ou Thawte), il n'est pas nécessaire d'ajouter des certificats au magasin de clés de confiance de certificats de l'agent Cisco UCS. En revanche, si la source de données utilise un certificat qui n'est pas signé par une autorité de certification courante, comme c'est le cas par défaut, le certificat doit être ajouté au magasin de clés de confiance pour permettre à l'agent de se connecter et de collecter des données.

Procédure

1. Copiez le fichier de certificat de votre source de données vers l'ordinateur de l'agent.
2. Sur l'ordinateur de l'agent, placez le fichier de certificat dans le répertoire de votre choix. Evitez tout écrasement des fichiers de certificat. Utilisez pour chaque certificat ajouté un nom de fichier et un libellé uniques.
3. Utilisez la commande `keytool` pour ajouter le certificat de source de données au magasin de clés de confiance de l'agent :

   ```
   keytool -import -noprompt -trustcacerts -alias CertificateAlias -file
   CertificateFile -keystore Truststore -storepass TruststorePassword
   ```

   Où

   CertificateAlias

   Référence unique pour chaque certificat ajouté au magasin de clés de confiance de l'agent ; par exemple, *datasource* est un alias approprié pour le certificat provenant de *datasource.example.com*.

CertificateFile
Nom et chemin d'accès complet au fichier de certificat de source de données Cisco UCS à ajouter au magasin de clés de confiance.

Truststore

Nom et chemin d'accès complet au fichier de la base de données de certificats de l'agent Cisco UCS. Utilisez le chemin et le nom de fichier suivants :

- Windows (64 bits) *rép_install*\tmaitm6_x64\kv6.truststore
- Linux (64 bits) : rép_install/lx8266/vm/etc/kv6.truststore

TruststorePassword

ITMFORVE est le mot de passe par défaut du magasin de clés de confiance de l'agent Cisco UCS. Pour modifier ce mot de passe, reportez-vous à la documentation relative à l'environnement d'exécution Java pour plus d'informations sur les outils à utiliser.

Important : Pour utiliser la commande `keytool`, le répertoire bin de l'environnement d'exécution Java doit être indiqué dans le chemin. Utilisez les commandes suivantes :

- Windows (64 bits) : `set PATH=%PATH%;rép_install\java\java70_x64\jre\bin`
- Linux (64 bits) : `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`

4. Après avoir ajouté tous les certificats de source de données, démarrez l'agent de surveillance.

Augmentation de la taille de segment de mémoire Java

Après avoir configuré l'agent Cisco UCS, si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java™.

Pourquoi et quand exécuter cette tâche

La taille de segment de mémoire par défaut du fournisseur de données Java est de 256 mégaoctets. Dans les environnements Cisco de grande taille, si les problèmes suivants surviennent, il peut s'avérer nécessaire d'augmenter la taille de segment de mémoire :

- Le fournisseur de données Java s'arrête en raison d'un problème `javacore` et crée un fichier nommé `javacore.`*`date.heure.numéro`*`.txt` dans le répertoire `CANDLEHOME\tmaitm6_x64`.
- Le fichier `javacore.`*`date.heure.numéro`*`.txt` contient la chaîne `java/lang/OutOfMemoryError`.

Procédure

- Windows Pour attribuer une valeur de 1 Go à la taille de segment de mémoire, procédez comme suit :
  1. Ouvrez le fichier `%CANDLE_HOME%\TMAITM6_x64\kv6_data_provider.bat`.
  2. Ajoutez la ligne suivante avant la ligne commençant par `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...` :
     `SET KV6_CUSTOM_JVM_ARGS=-Xmx1024m`
  3. Redémarrez l'agent.
- Linux Pour attribuer une valeur de 1 Go à la taille de segment de mémoire, procédez comme suit :
  1. Ouvrez le fichier `$CANDLEHOME/lx8266/vm/bin/kv6_data_provider.sh`.
  2. Ajoutez la ligne suivante avant la ligne commençant par `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...` :
     `KV6_CUSTOM_JVM_ARGS=-Xmx1024m`
  3. Redémarrez l'agent.

Configuration de la surveillance de Citrix Virtual Desktop Infrastructure

L'agent Citrix VDI permet de surveiller de manière centralisée vos ressources Citrix XenDesktop ou XenApp, y compris les groupes de distribution, les catalogues, les applications, les bureaux, les utilisateurs et les sessions. Avant de pouvoir utiliser l'agent, vous devez le configurer afin de collecter les données par le biais du contrôleur de distribution.

Avant de commencer

- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 41.

Tableau 41. Versions d'agent

Version d'agent	Documentation
8.1.4	Cloud APM 8.1.4
8.1.3.1, 8.1.3.2	IBM Performance Management 8.1.3 [1]

[1] Le lien ouvre une rubrique Knowledge Center sur site.

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Citrix VDI. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Citrix VDI.
- Vérifiez que les informations suivantes sont disponibles :
  - Nom d'hôte du contrôleur de distribution auquel vous prévoyez de vous connecter.
  - Nom d'utilisateur, mot de passe et domaine OData.
  - Nom d'utilisateur PowerShell, mot de passe, domaine, port PowerShell, type de vérification SSL et mécanisme d'authentification si vous activez l'extraction des événements du journal des événements Windows et des mesures PowerShell.
- Assurez-vous qu'un compte utilisateur d'opérateur d'agent dispose au moins des privilèges d'administrateur en lecture seule de Citrix. Voir la rubrique sur l'activation des privilèges d'administrateur en lecture seule de Citrix.
- La fonctionnalité d'extraction du journal des événements Windows est désormais disponible depuis la version 8.1.3.1 de l'agent Citrix VDI. Pour en bénéficier depuis l'ensemble des machines Desktop Delivery Controller (DDC) et Virtual Delivery Agent (VDA), vous devez activer l'accès PowerShell à distance pour le compte utilisateur qui a été spécifié lors de la configuration de l'instance de l'agent. Pour être sûr que l'agent pourra effectuer cette fonction, procédez comme suit :
  1. Connectez-vous à un ordinateur Windows en tant qu'utilisateur spécifié dans la configuration de l'instance d'agent.
  2. Exécutez la commande PowerShell suivante, où *vda_system* représente le nom d'une machine VDA sous tension :
     `Get-WinEvent -FilterHashtable @{ProviderName='Citrix*';LogName='Citrix*';StartTime=((Get-Date).AddDays(-10))} -ComputerName` *`système_vda`*
- Assurez-vous que les stratégies d'équilibrage de charge suivantes sont activées pour l'environnement surveillé :
  - Utilisation de l'UC
  - Utilisation du disque
  - Utilisation de la mémoire

  Vous pouvez configurer ces stratégies par le biais de l'application Citrix Studio.

Pourquoi et quand exécuter cette tâche

L'agent Citrix VDI est un agent multi-instance. Vous devez créer au moins une instance et démarrer l'instance d'agent manuellement.

La configuration des serveurs XenApp est identique à celle des serveurs XenDesktop. Si un nom ou une description de paramètre de configuration ne mentionne que «XenDesktop», il s'applique également à XenApp.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 273.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 277.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 276.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 277.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Activation des privilèges d'administrateur en lecture seule de Citrix

L'agent Citrix VDI requiert que le compte utilisateur d'opérateur d'agent dispose au moins des privilèges d'administrateur en lecture seule de Citrix.

Pourquoi et quand exécuter cette tâche

Pour effectuer ces étapes à distance depuis un ordinateur sur lequel le composant logiciel enfichable Citrix Delegated Admin PowerShell est installé, utilisez le paramètre `AdminAddress`. Par exemple, la commande à l'étape 2 deviendrait :
`New-AdminAdministrator -Name "`*`YOURDOMAIN`*`\`*`NewAdmin`*`" -AdminAddress "`*`controller1.YOURDOMAIN.com`*`"`.
Où *YOURDOMAIN* représente le nom du domaine réseau, *NewAdmin*, le compte utilisateur auquel les droits d'administration Citrix sont octroyés et *controller1.YOURDOMAIN.com*, le nom de domaine complet du serveur du site Citrix.

Procédure

1. Démarrez une session PowerShell avec un compte administrateur Citrix existant.
2. Chargez le composant logiciel enfichable Delegated Admin PowerShell pour gérer le site Citrix XenApp ou XenDesktop.

   ```
   (Add-PSSnapin Citrix.DelegatedAdmin.Admin.V1)
   ```

3. Ajoutez le compte utilisateur d'opérateur d'agent comme administrateur de site Citrix.

   `New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"` Où *YOURDOMAIN* représente le nom du domaine réseau et *NewAdmin*, le compte utilisateur auquel les droits d'administration Citrix sont octroyés.
4. Déterminez les rôles et portées disponibles à affecter à *NewAdmin*.

   ```
   Get-AdminRole
   Get-AdminScope
   ```
5. Affectez les rôles au compte utilisateur d'opérateur d'agent, notamment les droits d'administrateur en lecture seule.

   `Add-AdminRight -Administrator "YOURDOMAIN\NewAdmin" -Role "Read Only Administrator" -Scope "All"` Où
   - *YOURDOMAIN* représente le nom du domaine réseau.
   - *NewAdmin* représente le compte utilisateur auquel les droits d'administration Citrix sont octroyés.
   - *Read Only Administrator* représente le rôle d'administrateur de site Citrix que vous affectez.
   - *All* représente la portée d'administrateur de site Citrix que vous affectez.
6. Confirmez l'ajout et les modifications de l'administrateur.

   `Get-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"` Où *YOURDOMAIN* représente le nom du domaine réseau et *NewAdmin*, le compte utilisateur auquel les droits d'administration Citrix sont octroyés.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Citrix VDI sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Citrix Virtual Desktop Infrastructure**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `vdi_inst2`.

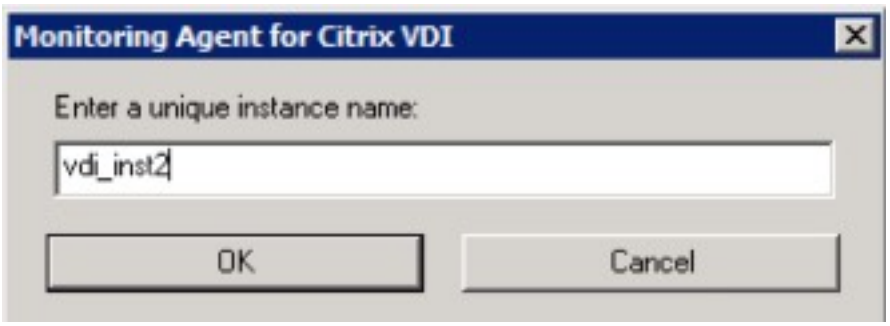


Figure 13. Fenêtre de saisie d'un nom d'instance unique.

4. Cliquez sur **Suivant** dans la fenêtre du nom d'instance de l'agent.

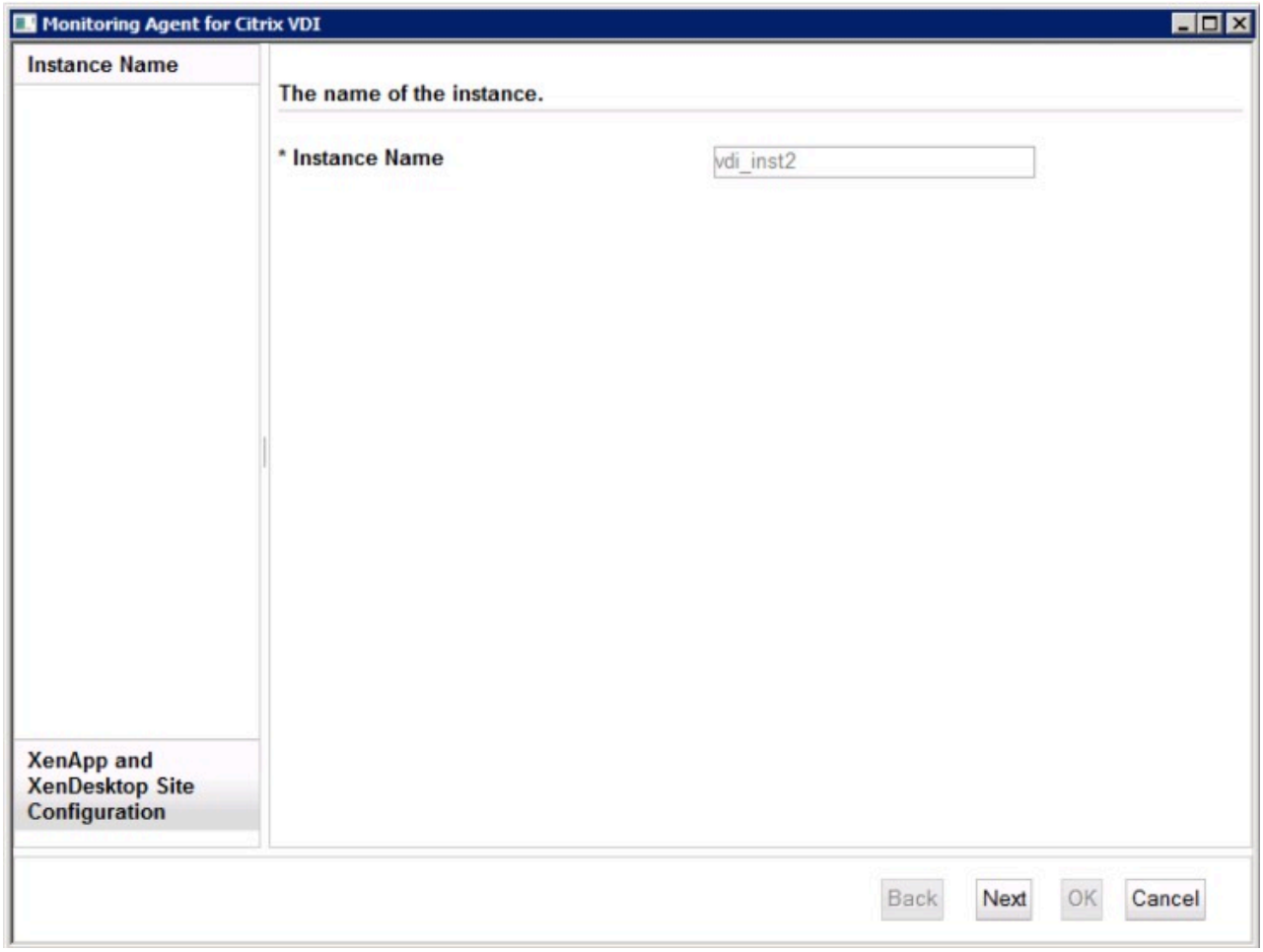


Figure 14. Fenêtre du nom d'instance de l'agent.

5. Entrez les paramètres du modèle d'instance **Configuration de site XenApp et XenDesktop**.

   Remarque : Cette section ne décrit pas la configuration de l'instance de site XenApp ou XenDesktop. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut lorsque vous ajoutez les véritables configurations d'instance de site XenApp ou XenDesktop à l'étape 6.
   Pour obtenir une description de chaque paramètre de configuration, voir tableau 42, à la page 278.

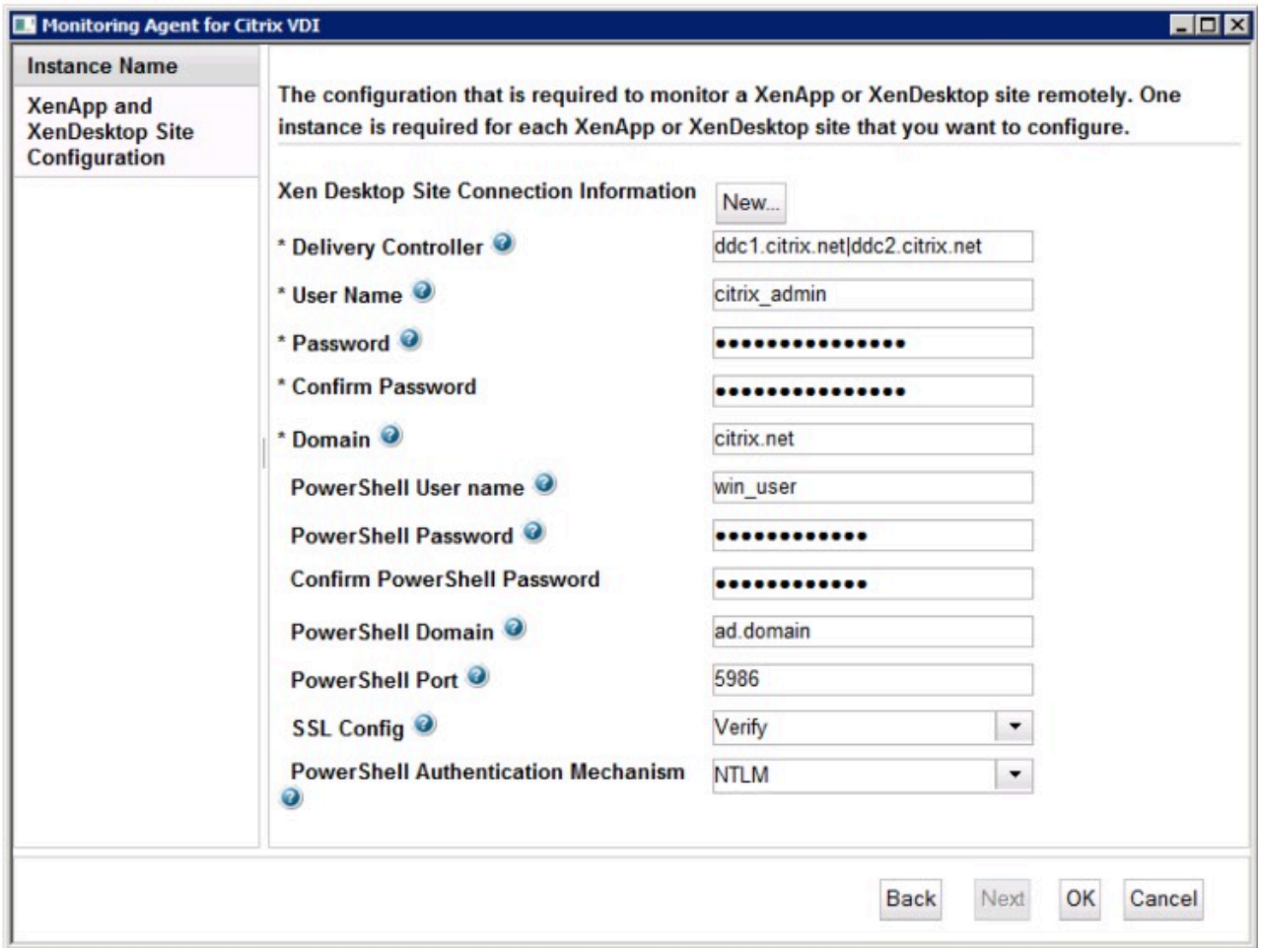


Figure 15. Fenêtre de spécification des paramètres du modèle d'instance de site XenApp ou XenDesktop

6. Appuyez sur **Nouveau** et entrez les paramètres d'instance de site XenApp ou XenDesktop, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 42, à la page 278.

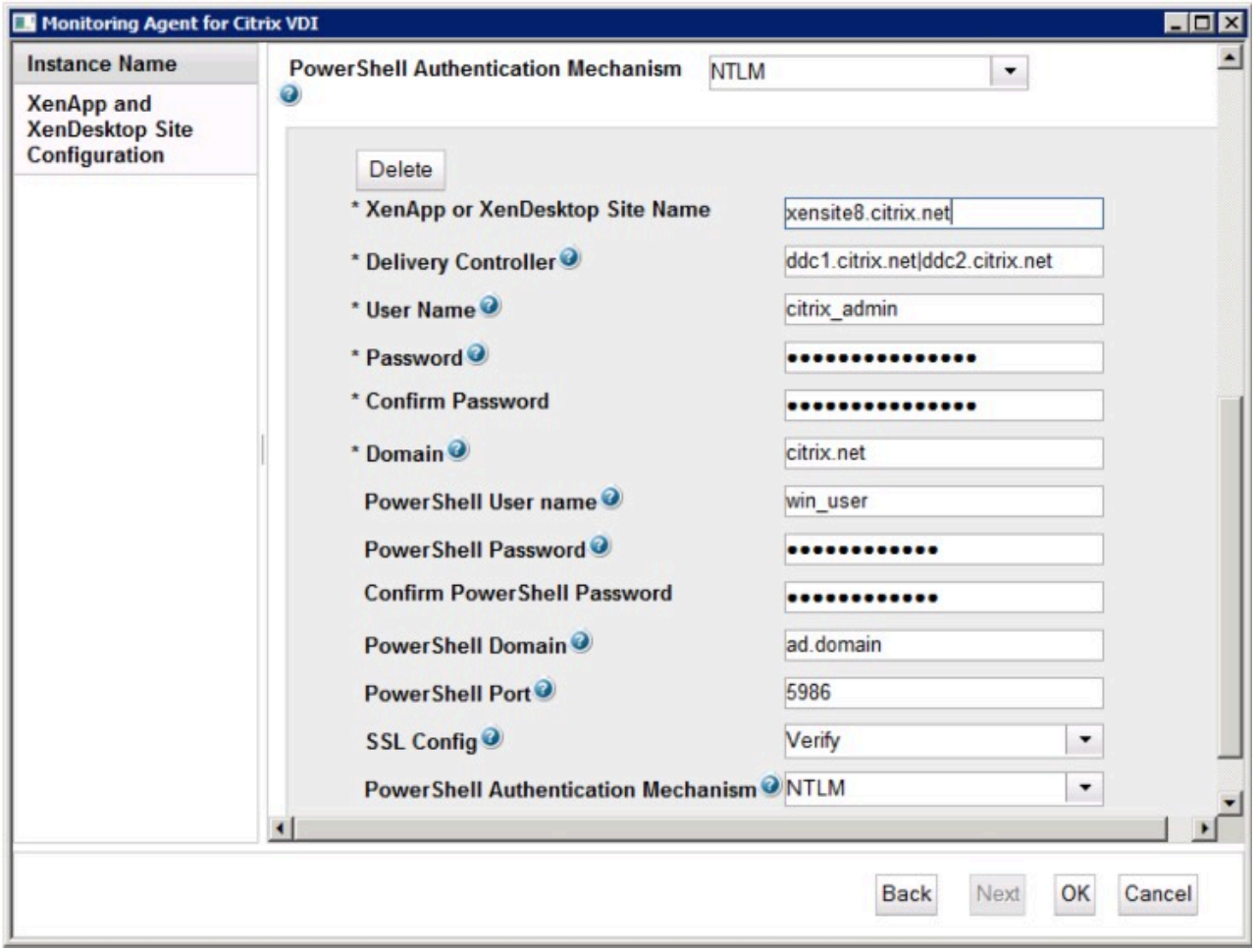


Figure 16. Fenêtre de spécification des paramètres d'instance de site XenApp ou XenDesktop

Remarque : Le paramètre **`Nom d'utilisateur PowerShell`** et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 280. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.

Remarque : Vérifiez que les paramètres de **`configuration SSL`** et du **`mécanisme d'authentification PowerShell`** sont définis correctement pour chaque nouvelle instance de site XenApp ou XenDesktop. Un incident entraîne la définition des valeurs par défaut et non des valeurs de modèle.

7. Cliquez sur **OK** pour terminer la configuration.
8. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent Citrix VDI, vous devez le configurer pour pouvoir le démarrer. Si l'agent Citrix VDI est installé sur une machine Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Citrix VDI en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   rép_install/bin/citrixvdi-agent.sh
   config *nom_instance*

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Citrix VDI», à la page 278.

   Remarque : Le paramètre **Nom d'utilisateur PowerShell** et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 280. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.

3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/citrixvdi-agent.sh
   start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01
   ```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Configurez l'agent Citrix VDI en mode silencieux :

1. Ouvrez le fichier `citrixvdi_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
   - Linux *rép_install*/samples/citrixvdi_silent_config.txt

     Par exemple, `/opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt`
   - Windows *rép_install*\samples\citrixvdi_silent_config.txt

     Par exemple, `C:\IBM\APM\samples\citrixvdi_silent_config.txt`

   où *rép_install* représente le chemin d'installation de l'agent.
2. Dans le fichier `citrixvdi_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Citrix VDI».

Remarque : Le paramètre **Nom d'utilisateur PowerShell** et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 280. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.

3. Sauvegardez et fermez le fichier `citrixvdi_silent_config.txt`, puis exécutez la commande suivante :
   - Linux *rép_install*`/bin/citrixvdi-agent.sh config` **nom_instance** *rép_install*`/samples/citrixvdi_silent_config.txt`

     Par exemple, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01 /opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt**
   - Windows *rép_install*`\bin\citrixvdi-agent.bat config` **nom_instance** *rép_install*`\samples\citrixvdi_silent_config.txt`

     Par exemple, **C:\IBM\APM\bin\citrixvdi-agent.bat config vdi_inst01 C:\IBM\APM\samples\citrixvdi_silent_config.txt**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*`/bin/citrixvdi-agent.sh start` **nom_instance**

     Par exemple, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01**
   - Windows *rép_install*`\bin\citrixvdi-agent.bat start` **nom_instance**

     Par exemple, **C:\IBM\APM\bin\citrixvdi-agent.bat start vdi_inst01**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Paramètres de configuration de l'agent Citrix VDI

Les paramètres de configuration de l'agent Citrix VDI sont regroupés dans un tableau.

1. Paramètres de l'agent Citrix VDI - Paramètres d'environnement de l'agent Citrix VDI.

Tableau 42. Paramètres de l'agent Citrix VDI

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du site XenApp ou XenDesktop	Indiquez un nom pour identifier l'instance d'agent du site XenApp ou XenDesktop. Par exemple, *vdi_inst2* **Remarque :** cet alias vous permet de représenter l'instance de l'agent du serveur WebLogic avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.	Chacun des paramètres suivants doit avoir un suffixe de nom d'instance qui est le même pour chaque paramètre d'une instance d'agent. Les nouvelles instances d'agent doivent utiliser un nom d'instance unique pour son jeu de paramètres. Par exemple, une instance d'agent peut utiliser *.vdi1* et une autre instance d'agent peut utiliser *.vdi2* à la place de *.nom_instance* dans les noms de paramètres ci-après.
Contrôleur de distribution	Nom d'hôte ou adresse IP du contrôleur de distribution. Si plusieurs DDC sont configurés dans un cluster, une liste de contrôleurs de distribution séparés par un caractère '|' peut être fournie.	**KVD_XDS_DELIVERY_CONTROLLER.instance_name**

Tableau 42. Paramètres de l'agent Citrix VDI (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom d'utilisateur	Nom d'utilisateur utilisé pour s'authentifier avec l'API OData sur le contrôleur de distribution XenApp ou XenDesktop spécifié.	**KVD_XDS_ODATA_USERNAME.instance_name**
Mot de passe	Mot de passe utilisé pour s'authentifier avec l'API OData sur le contrôleur de distribution XenApp ou XenDesktop spécifié.	**KVD_XDS_ODATA_PASSWORD.instance_name**
Domaine	Domaine utilisé pour s'authentifier avec l'API OData sur le contrôleur de distribution XenApp ou XenDesktop spécifié.	**KVD_XDS_ODATA_DOMAIN.instance_name**
Nom d'utilisateur PowerShell	Nom d'utilisateur utilisé pour s'authentifier pour les appels PowerShell aux machines VDA et DDC distantes. **Remarque :** ce paramètre et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 280. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.	**KVD_XDS_POWERSHELL_USERNAME.instance_name**
Mot de passe PowerShell	Mot de passe associé au nom d'utilisateur PowerShell fourni.	**KVD_XDS_POWERSHELL_PASSWORD.instance_name**
Domaine PowerShell	Domaine associé au nom d'utilisateur PowerShell fourni.	**KVD_XDS_POWERSHELL_DOMAIN.instance_name**
Port PowerShell	Pour SSL ouvert pour être utilisé par WinRm. Les ports de connexion distants par défaut de PowerShell sont 5985 pour HTTP et 5986 pour HTTPS.	**KVD_XDS_POWERSHELL_PORT.instance_name**
Exigence SSL	Choisissez l'option SSL requise pour votre environnement.	**KVD_XDS_SSL_CONFIG.instance_name** Les valeurs possibles sont les suivantes : **KVD_XDS_SSL_CONFIG_VERIFY** Vérification **KVD_XDS_SSL_CONFIG_NOVERIFY** Pas de vérification **KVD_XDS_SSL_CONFIG_NOSSL** Pas de couche SSL

Tableau 42. Paramètres de l'agent Citrix VDI (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Mécanisme d'authentification PowerShell	Définit le type d'authentification utilisé pour créer des données d'identification afin d'extraire les informations de systèmes distants avec PowerShell.	**KVD_XDS_POWERSHELL_AUTH_MECH.instance_name** Les valeurs possibles sont les suivantes : **KVD_XDS_POWERSHELL_BASIC** De base **KVD_XDS_POWERSHELL_CREDSSP** CredSSP **KVD_XDS_POWERSHELL_NTLM** NTLM **KVD_XDS_POWERSHELL_DEFAULT** Valeur par défaut **KVD_XDS_POWERSHELL_DIGEST** Prétraitement **KVD_XDS_POWERSHELL_KERBEROS** Kerberos **KVD_XDS_POWERSHELL_NEGOTIATE** Négociation

Activation de la surveillance des événements Windows et des mesures PowerShell

Activez la surveillance des événements Windows et des mesures PowerShell à l'aide de cette procédure. La surveillance de ces données peut avoir un impact considérable sur les performances du système géré.

Avant de commencer

Vérifiez que les paramètres de configuration PowerShell de l'agent sont définis.

Pourquoi et quand exécuter cette tâche

Une ou plusieurs des variables d'environnement avancées ci-après doivent être activées pour que l'agent puisse surveiller les événements Windows et les mesures PowerShell.

GET_SESSION_LATENCY
Indique si le temps d'attente de la session et la durée de la boucle sont extraits à distance de la machine VDA connectée de PowerShell.

GET_VDA_MACHINE_METRICS_REMOTELY
Indique si les mesures de la machine VDA sont extraites à distance de PowerShell.

RETRIEVE_WINDOWS_EVENTS
Indique si les événements du journal des événements Windows sont extraits de PowerShell à partir des machines VDA et DDC Windows.

Procédure

1. Accédez au répertoire d'installation de l'agent Citrix VDI :
   - Linux *rép_install*/config
   - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent.

2. Editez le fichier de configuration de l'agent Citrix VDI pour définir une ou plusieurs des variables *GET_SESSION_LATENCY*, *GET_VDA_MACHINE_METRICS_REMOTELY* et *RETRIEVE_WINDOWS_EVENTS* sur `true`.
   - Linux `vd.environment`
   - Windows `KVDENV_nom_instance`

   où *nom_instance* représente le nom de l'instance d'agent.
3. Redémarrez l'agent.

   Important : Pour que ces paramètres soient définis par défaut pour toutes les nouvelles instances d'agent, définissez-les sur `true` dans les fichiers du modèle de configuration :
   - Linux Ce paramètre a déjà été défini par défaut pour les nouvelles instances d'agent en éditant `vd.environment` à l'étape 2.
   - Windows `KVDENV`

Exemple

```
GET_SESSION_LATENCY=true
GET_VDA_MACHINE_METRICS_REMOTELY=true
RETRIEVE_WINDOWS_EVENTS=true
```

Configuration de la surveillance DataPower

Pour surveiller les dispositifs DataPower, vous devez effectuer certaines tâches de configuration sur vos dispositifs, puis configurer Monitoring Agent for DataPower.

Conseil : Cliquez sur APM v8: Configuring DataPower monitoring in IBM APM pour regarder une vidéo concernant le processus de configuration de base de la surveillance DataPower.

Configuration des dispositifs DataPower

Pour pouvoir configurer Monitoring Agent for DataPower, vous devez effectuer certaines tâches de configuration sur vos dispositifs.

Conseil : Pour plus d'informations sur les dispositifs DataPower pris en charge, consultez l'onglet Prerequisites sur la page des rapports de compatibilité des produits logiciels.

Vous pouvez surveiller les dispositifs DataPower à trois niveaux différents. Configurez les trois niveaux en fonction de vos besoins sur chaque dispositif DataPower que vous voulez surveiller pour afficher les données de dispositif DataPower dans la console Cloud APM.

1. Surveillance des ressources

   Pour définir des données de surveillance, telles que l'utilisation des ressources, le débit et les statistiques de connexion, activez la surveillance des ressources. Pour plus d'informations, voir «Surveillance des ressources», à la page 282.
2. Suivi des transactions de middleware

   Pour afficher des données de surveillance pour des transactions, telles que les informations détaillées, le volume et les dépendances des transactions, activez le suivi de transaction de middleware. Pour plus d'informations, voir «Suivi des transactions de middleware», à la page 283.
3. Suivi des transactions de niveau instance du dispositif DataPower

   Pour afficher les données de surveillance pour des transactions dans les topologies des instances, configurez le suivi des transactions de niveau instance du dispositif DataPower. Pour plus d'informations, voir «Suivi des transactions de niveau instance du dispositif DataPower», à la page 284.

Important : Assurez-vous que l'ID utilisateur possède les droits appropriés pour configurer le dispositif DataPower. Vous pouvez entrer `*/*/*?Access=r` dans la zone **Access profile** pour l'ID utilisateur utilisé pour configurer le dispositif DataPower. Utilisez ensuite cet ID utilisateur pour configurer le dispositif DataPower.

Exportation du certificat public

Si le profil de proxy SSL est activé sur l'interface de gestion XML du dispositif DataPower, vous devez exporter le certificat public utilisé par l'interface de gestion XML du dispositif DataPower sur la machine qui exécute l'agent DataPower.

Procédure

1. Pour télécharger le certificat cryptographique utilisé par l'interface de gestion XML du dispositif DataPower, par exemple `pubcert:///mycert.pem`, cliquez sur **Administration** > **Main** > **File Management** et enregistrez le certificat sur la machine qui exécute l'agent DataPower.
2. Lorsque vous configurez l'agent DataPower, vous avez la possibilité de spécifier la zone **SSL Proxy Profile**. Entrez le chemin d'accès absolu au certificat public.

   Remarque : Lorsque plusieurs passerelles multiprotocole sont ajoutées, vous devez répéter ces étapes.

Surveillance des ressources

Le premier niveau de surveillance disponible sur un dispositif DataPower est d'activer le contrôle des ressources, telles que la gestion SOAP, les statistiques et les taux de transaction.

L'opération dans l'interface utilisateur de DataPower Gateway décrite dans les tâches de configuration suivantes s'applique à DataPower Gateway Version 7.5.1 et antérieure. Si la version de DataPower Gateway que vous utilisez est postérieure à 7.5.1, vous pouvez cliquer sur le point d'interrogation situé dans le coin supérieur droit de l'interface utilisateur et sélectionner **WebGUI** pour revenir à la version antérieure de l'interface utilisateur. Suivez ensuite les instructions pour exécuter les tâches de configuration du dispositif DataPower.

Activation de la gestion SOAP :

Si vous souhaitez que l'agent DataPower collecte des données des dispositifs DataPower, vous devez configurer l'interface de gestion XML et activer la gestion de SOAP.

Procédure

Pour activer SOAP :

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Cliquez sur **Objects** > **Device Management** > **XML Management Interface**.

   Remarque : Vérifiez que l'état administratif est activé.
3. Pour **Port Number**, indiquez le numéro de port sur lequel l'agent DataPower écoute les rapports de notification. Le numéro de port par défaut est 5550.
4. Pour **Enabled Services**, vérifiez que **SOAP Management** est sélectionné.

Activation des statistiques :

Si vous souhaitez que l'agent DataPower collecte des données à partir des dispositifs DataPower, les statistiques doivent être activées.

Procédure

Pour activer les statistiques, procédez comme suit :

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.

2. Cliquez sur **Administration** > **Device** > **Statistics Settings**.
3. Activez **Statistics Settings** et cliquez sur **Apply**.

Activation du débit de transaction :

Si vous souhaitez que l'agent DataPower collecte des données à partir des dispositifs DataPower, le débit de transaction doit être activé.

Procédure

Pour activer le débit de transaction, procédez comme suit :

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Sélectionnez le domaine `default`.
3. Cliquez sur **Status** > **Connection** > **Transaction Rate**.
4. Si le message **Statistics is currently disabled** s'affiche, cliquez sur **disabled** et définissez **Administrative state** sur **enabled** dans les paramètres des statistiques.
5. Si vous disposez de plusieurs domaines, cliquez sur **Show All Domains** et répétez les étapes 3-4 pour activer le débit de transaction pour tous les domaines applicables.
6. Cliquez sur **Apply**.

Suivi des transactions de middleware

Le deuxième niveau de surveillance disponible pour un dispositif DataPower consiste à afficher le suivi des transactions de middleware dans les espaces de travail.

L'opération dans l'interface utilisateur de DataPower Gateway décrite dans les tâches de configuration suivantes s'applique à DataPower Gateway Version 7.5.1 et antérieure. Si la version de DataPower Gateway que vous utilisez est postérieure à 7.5.1, vous pouvez cliquer sur le point d'interrogation situé dans le coin supérieur droit de l'interface utilisateur et sélectionner **WebGUI** pour revenir à la version antérieure de l'interface utilisateur. Suivez ensuite les instructions pour exécuter les tâches de configuration du dispositif DataPower.

Le suivi des transactions des trafics SOAP et REST par l'intermédiaire du dispositif DataPower est pris en charge. Le suivi des transactions DataPower prend en charge SOAP à l'aide des fichiers `store:///soapreq.xsl`, `store:///soaprsp.xsl` et `store:///soaperror.xsl`. Ces fichiers XSL instrumentent le proxy de service Web pour ajouter et générer des rapports sur `kd4:KD4SoapHeaderV2` dans l'enveloppe SOAP.

Outre les fichiers `soap*.xsl`, le suivi des transactions DataPower inclut également les fichiers `apm_req.xsl`, `apm_rsp.xsl` et `apm_error.xsl`, qui prennent en charge les demandes HTTP entrantes contenant `ARM_CORRELATOR: HTTP Header`, ou une enveloppe SOAP contenant `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. Le proxy de service Web met à jour ou définit la demande sortante de sorte à contenir `ARM_CORRELATOR: HTTP Header` et supprime les corrélateurs SOAP.

Remarque : Si des dispositifs DataPower sont ajoutés à une application métier et que le dispositif transporte le trafic pour plusieurs applications, lorsque le suivi des transactions est activé, la topologie d'application affichée pour ces applications métier comprend les chemins vers les noeuds pour toutes les applications.

Configuration de Web Service Management :

Procédez comme suit pour chaque dispositif DataPower dont vous souhaitez afficher les données de suivi.

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Sélectionnez le domaine `default`.

3. Recherchez `XML Management Interface`. Définissez les valeurs suivantes et cliquez sur **Apply**.
   - Dans l'onglet **Main**, section **Enabled services**, activez **WS-Management endpoint**
4. Recherchez `Web Services Management Agent`. Définissez les valeurs suivantes et cliquez sur **Apply**.
   - Définissez **Administrative state** sur **enabled**
   - Définissez **Capture Mode** sur **None**
   - Définissez **Buffering Mode (deprecated)** sur **Discard**
5. Configurez le proxy de service Web ou la passerelle multiprotocole comme décrit dans les rubriques suivantes.

Configuration du proxy de service Web :

Procédez comme suit pour chaque proxy de service Web dont vous souhaitez afficher les données de suivi.

Procédure

1. Sélectionnez le domaine dont fait partie le proxy de service Web.
2. Dans l'onglet **Proxy Settings**, définissez les valeurs suivantes et cliquez sur **Apply** :
   - Définissez **Monitor via Web Services Management Agent** sur **on**
3. Pour signaler les fautes SOAP, désactivez le traitement d'erreur et activez la génération de rapports d'erreurs dans la console Cloud APM : dans l'onglet **Advanced Proxy Settings**, définissez **Process HTTP Errors** sur `off` et cliquez sur **Apply**.

Configuration de la passerelle multiprotocole :

Procédez comme suit pour chaque passerelle multiprotocole dont vous souhaitez afficher les données de suivi des transactions.

Procédure

1. Sélectionnez le domaine dont fait partie la passerelle multiprotocole.
2. Dans l'onglet **Advanced** de la passerelle multiprotocole, définissez les valeurs suivantes et cliquez sur **Apply** :
   - Définissez **Monitor via Web Services Management Agent** sur **on**
   - Si le serveur Web utilise des redirections, définissez **Follow Redirects** sur **off**. Définissez ensuite **Rewrite Location URL** sur **on**.
3. Si vous surveillez une passerelle multiprotocole avec un type de réponse ou un type de demande défini sur `Non-XML`, vous devez définir une stratégie de passerelle multiprotocole dont les règles couvrent à la fois la direction Client to Server et Server to Client. Si la stratégie d'une passerelle multiprotocole non XML ne possède aucune règle, aucun trafic n'est capturé par l'agent Web Services Management ou par une sonde de débogage DataPower (si activée).
4. Pour propager le Code de réponse HTTP du serveur d'arrière-plan et signaler les fautes SOAP, sous l'onglet **Advanced Settings**, définissez **Process Backend Errors** sur `off` et cliquez sur **Apply**.

Suivi des transactions de niveau instance du dispositif DataPower

Le troisième niveau de surveillance disponible pour un dispositif DataPower consiste à afficher ses données dans des topologies d'instance.

L'opération dans l'interface utilisateur de DataPower Gateway décrite dans les tâches de configuration suivantes s'applique à DataPower Gateway Version 7.5.1 et antérieure. Si la version de DataPower Gateway que vous utilisez est postérieure à 7.5.1, vous pouvez cliquer sur le point d'interrogation situé dans le coin supérieur droit de l'interface utilisateur et sélectionner **WebGUI** pour revenir à la version antérieure de l'interface utilisateur. Suivez ensuite les instructions pour exécuter les tâches de configuration du dispositif DataPower.

Configuration des transformations :

Procédez comme suit sur chaque dispositif DataPower que vous voulez afficher dans les topologies d'instance.

Pourquoi et quand exécuter cette tâche

Pour IBM Performance Management V8.1.2 Fix Pack 1, le suivi des transactions du trafic SOAP par l'intermédiaire du dispositif DataPower est pris en charge. Le suivi des transactions DataPower prend en charge SOAP à l'aide des fichiers `store:///soapreq.xsl`, `store:///soaprsp.xsl` et `store:///soaperror.xsl`. Ces fichiers XSL instrumentent le proxy de service Web pour ajouter et générer des rapports sur `kd4:KD4SoapHeaderV2` dans l'enveloppe SOAP.

Pour IBM Performance Management V8.1.3 et ultérieure, le suivi des transactions du trafic REST par l'intermédiaire du dispositif DataPower est également pris en charge. Outre les fichiers `soap*.xsl`, le suivi des transactions DataPower inclut également les fichiers `apm_req.xsl`, `apm_rsp.xsl` et `apm_error.xsl`, qui prennent en charge les demandes HTTP entrantes contenant `ARM_CORRELATOR: HTTP Header`, ou une enveloppe SOAP contenant `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. Le proxy de service Web met à jour ou définit la demande sortante de sorte à contenir `ARM_CORRELATOR: HTTP Header` et supprime les corrélateurs SOAP.

L'agent DataPower prend en charge le suivi des transactions pour le trafic SOAP via le dispositif DataPower, le trafic REST via le dispositif DataPower et le trafic entre DataPower et WebSphere MQ.

- Pour activer le suivi des transactions pour le trafic SOAP et REST via le dispositif DataPower, appliquez `apm_req.xsl`, `apm_rsp.xsl` et `apm_error.xsl`, qui prennent en charge les demandes HTTP entrantes contenant `ARM_CORRELATOR: HTTP Header`, ou une enveloppe SOAP contenant `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. Le proxy de service Web met à jour ou définit la demande sortante de sorte à contenir `ARM_CORRELATOR: HTTP Header` et supprime les corrélateurs SOAP.
- Pour activer le suivi des transactions entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez les fichiers `apm_req_MQ.xsl`, `apm_rsp_MQ.xsl` et `apm_error_MQ.xsl`. Le suivi des transactions pour le trafic SOAP et REST est également activé automatiquement après avoir appliqué ces fichiers.

Procédure

Pour suivre le trafic REST et activer le suivi des transactions entre DataPower et WebSphere MQ, procédez comme suit :

1. Téléchargez les fichiers à partir de l'emplacement suivant :
   - Pour les systèmes Linux, `/opt/ibm/apm/agent/`*`lx8266`*`/bn/bin`
   - Pour les systèmes AIX, `/opt/ibm/apm/agent/`*`aix536`*`/bn/bin`
2. Transférez les fichiers XSL vers chaque dispositif DataPower que vous voulez surveiller dans le cadre de la Pile d'intégration IBM.
3. Configurez le proxy de service Web ou la passerelle multiprotocole comme décrit dans les rubriques suivantes.
4. Configurez chaque domaine que vous voulez surveiller comme suit :
   a. Sélectionnez le domaine dans la liste déroulante de l'en-tête DataPower Gateway.
   b. Dans le navigateur du panneau de configuration, sélectionnez **Objects** > **Device Management** > **Web Services Management Agent**.
   c. Définissez **Buffering Mode (deprecated)** sur `Discard`.
   d. Cliquez sur **Appliquer**.

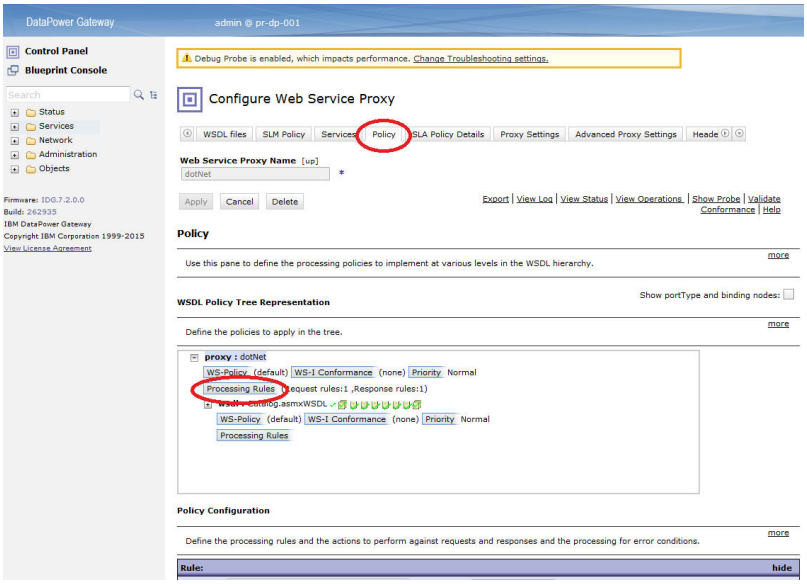
Configuration du proxy de service Web :

Procédez comme suit sur chaque proxy de service Web que vous voulez afficher dans les topologies d'instance.

Procédure

Dans l'interface graphique Web, procédez comme suit pour chaque proxy de service Web que vous voulez surveiller :

1. Sur la page **Configure Web Service Proxy**, sélectionnez le nom du proxy de service Web à configurer.
2. Dans l'onglet **Policy**, développez **proxy : *domaine*** et cliquez sur **Processing Rules**.

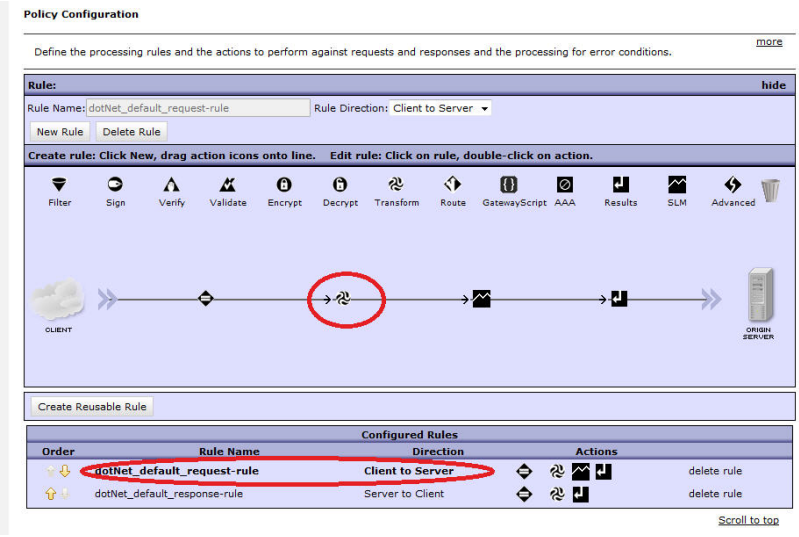


3. Dans la section **Policy Configuration**, sélectionnez une règle `Client to Server` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.

      Remarque :

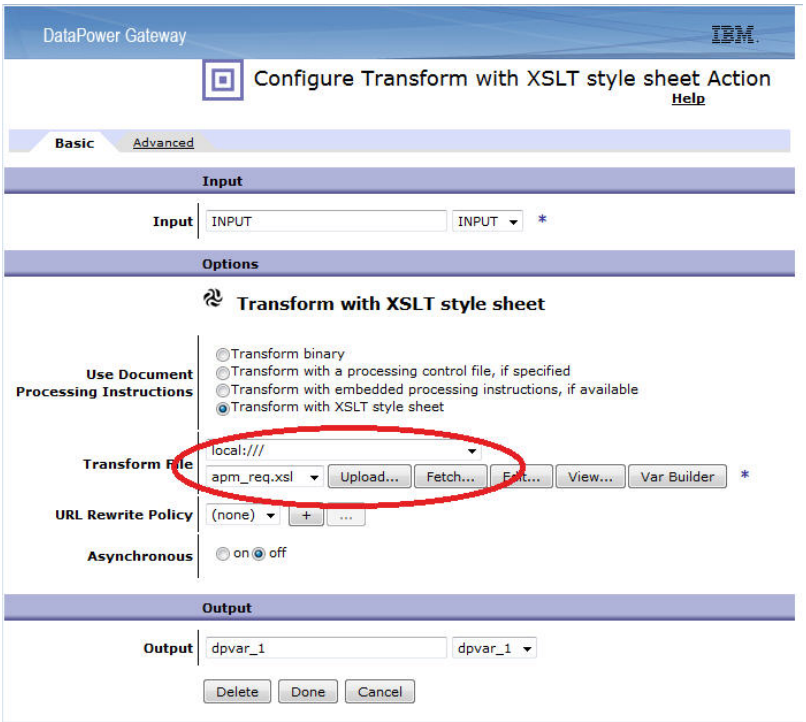
      1) Si une règle `Client to Server` existe déjà, ajoutez-y le noeud de transformation.
      2) Si la règle `Client to Server` a un noeud Authentification, Autorisation et Audit (AAA), veillez à ce que le noeud de transformation qui inclut le fichier xslt de l'agent DataPower précède le noeud AAA.

   b. Cliquez deux fois sur la transformation pour l'éditer.



c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_req.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

   Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.



   Conseil : Pour configurer une règle `Client to Server` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_req_MQ.xsl` à la place du fichier `apm_req.xsl` au cours de cette étape.

d. Cliquez sur **Done**.

4. Dans la section **Policy Configuration**, répétez l'étape 3 pour configurer une règle `Server to Client` ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.
   b. Cliquez deux fois sur la transformation pour l'éditer.

c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_rsp.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

   Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

   Conseil : Pour configurer une règle `Server to Client` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_rsp_MQ.xsl` à la place du fichier `apm_rsp.xsl` au cours de cette étape.

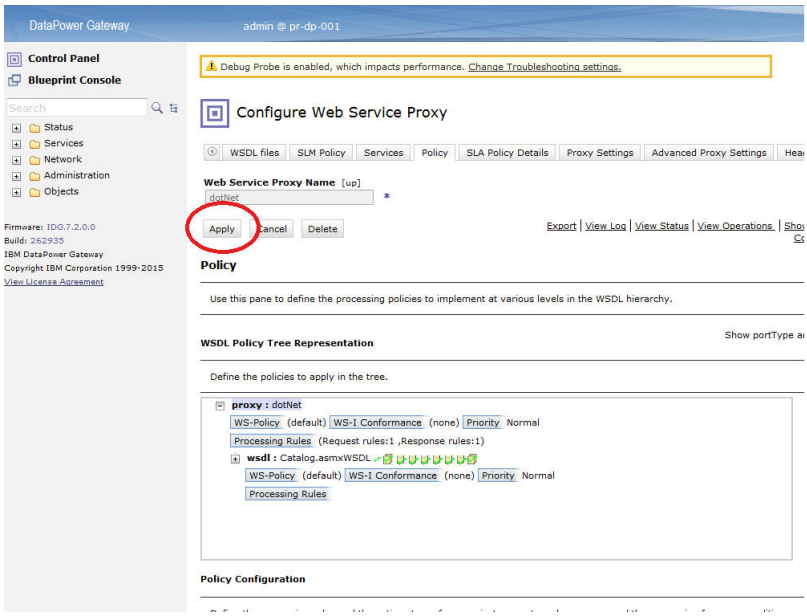
d. Cliquez sur **Done**.

5. Dans la section **Policy Configuration**, répétez l'étape 3 pour configurer une règle `Error` ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.
   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_error.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `error` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_error_mq.xsl` à la place du fichier `apm_error.xsl` au cours de cette étape.

   d. Cliquez sur **Done**.
6. Sur la page **Configure Web Service Proxy**, cliquez sur **Apply**.



Configuration de la passerelle multiprotocole :

Procédez comme suit sur chaque passerelle multiprotocole que vous voulez afficher dans les topologies d'instance.

Procédure

Dans l'interface graphique Web, procédez comme suit pour chaque passerelle multiprotocole que vous voulez surveiller.

1. Sur la page **Configure Multi-Protocol Gateway**, cliquez sur le nom de la passerelle multiprotocole que vous voulez configurer.
2. Sur la page **Multi-Protocol Gateway Policy**, configurez la règle. Cliquez sur **...**.
3. Sur la page **Configure Multi-Protocol Gateway Style Policy**, sélectionnez une règle `Client to Server` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.

      Remarque :
      1) Si une règle `Client to Server` existe déjà, ajoutez-y le noeud de transformation.
      2) Si la règle `Client to Server` a un noeud Authentification, Autorisation et Audit (AAA), veillez à ce que le noeud de transformation qui inclut le fichier xslt de l'agent DataPower précède le noeud AAA.
   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_req.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `Client to Server` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_req_MQ.xsl` à la place du fichier `apm_req.xsl` au cours de cette étape.
   d. Cliquez sur **Terminé**.
4. Sur la page **Configure Multi-Protocol Gateway Style Policy**, sélectionnez une règle `Server to Client` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.
   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_rsp.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `Server to Client` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_rsp_MQ.xsl` à la place du fichier `apm_rsp.xsl` au cours de cette étape.
   d. Cliquez sur **Terminé**.
5. Sur la page **Configure Multi-Protocol Gateway Style Policy**, sélectionnez une règle `Error` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.
   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_error.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `error` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_error_mq.xsl` à la place du fichier `apm_error.xsl` au cours de cette étape.
   d. Cliquez sur **Terminé**.
6. Sur la page **Configure Multi-Protocol Gateway Style Policy**, dans l'onglet **Advanced**, définissez **Monitor via Web Services Management Agent** sur **on** et cliquez sur **Apply**.

7. Cliquez sur **Apply**.

Que faire ensuite

Dans certains cas, l'ajout de transformations au Suivi des transactions amène DataPower à modifier la valeur des en-têtes Content-Type HTTP. De ce fait, vous pouvez voir des pages Web avec des images qui ne se chargent pas ou des fichiers binaires qui s'affichent avec du texte HTML déformé.

Le comportement de DataPower change lorsqu'il compare une règle ne comportant pas de transformations XSL à une règle comportant une ou plusieurs transformations XSL. Si le service traite des messages codés en MIME, MTOM, XOP ou autre, ce comportement peut être souhaité. Sinon, modifiez votre configuration DataPower en conséquence afin d'éviter ce comportement.

Pour empêcher DataPower de modifier l'en-tête Content-Type HTTP, définissez la variable var://service/mpgw/proxy-content-type dans chaque règle affectée :

1. Faites glisser un objet avancé vers la règle.
2. Cliquez deux fois sur l'objet avancé pour l'éditer.
3. Sélectionnez **Définir variable** et cliquez sur **Suivant**.
4. Entrez le nom de variable `service/mpgw/proxy-content-type` et la valeur de variable 1, puis cliquez sur **Terminé**.
5. Appliquez les modifications apportées à la configuration de service et de règle.
6. Répétez les étapes 1 à 5 pour chaque règle affectée.

Configuration de l'agent DataPower

L'Monitoring Agent for DataPower fournit un point central de surveillance des dispositifs DataPower dans votre environnement d'entreprise. Il permet d'identifier et de recevoir des notifications sur les problèmes courants liés aux dispositifs. L'agent fournit également des informations sur les performances, les ressources et la charge de travail des dispositifs.

Pourquoi et quand exécuter cette tâche

L'agent DataPower est un agent à plusieurs instances ; vous devez créer la première et lancer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*pc* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères.

Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous spécifiez `DataPower` comme nom d'instance, votre nom de système géré est `DataPower:hostname:BN`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.

Pour chaque dispositif DataPower de production, configurez une instance. Si vos dispositifs DataPower ne sont pas utilisés en production ou qu'ils sont petits, vous ne pouvez configurer qu'une instance d'agent pour les surveiller. Vous pouvez exécuter plusieurs instances sur la même machine. Vous pouvez exécuter le script de configuration pour créer une instance et modifier n'importe quels paramètres de configuration. Vous pouvez éditer le fichier de réponses silencieux de l'agent avant d'exécuter le script afin d'éviter les invites et les réponses qui sont requises.

Procédure

Pour configurer l'agent DataPower, suivez l'une des procédures ci-dessous :

- Linux AIX Pour configurer l'agent en répondant à des invites, procédez comme suit :
  1. Accédez au répertoire *rép_install*/bin, où *rép_install* correspond au répertoire d'installation de l'agent DataPower.
  2. Exécutez la commande `./datapower-agent.sh config` *nom_instance*.
     Sélectionnez un *nom_instance* unique sur le serveur.
  3. A l'invite d'édiction des paramètres de l'agent DataPower, entrez 1 pour continuer.
  4. A l'invite d'édition des **informations sur le système géré**, entrez l'une des options suivantes :
     - `1=Add`
     - `2=Edit`
     - `3=Del`
     - `4=Next`
     - `5=Exit`

     Si vous configurez une instance d'agent DataPower pour la première fois sur votre système, le message `No 'DataPower Appliances' settings available` s'affiche. Entrez `1` pour ajouter un paramètre DataPower Appliances. L'option par défaut est `5=Exit`.
  5. Entrez les propriétés du dispositif DataPower :

     Nom du système géré
     Entrez le nom du système géré de l'agent dans **Nom du système géré**.

     Sélectionnez un **Nom de système géré** unique pour toutes les instances de l'agent et permettant d'identifier facilement un dispositif. Ce nom ne doit contenir que des caractères alphanumériques, par exemple, le nom d'hôte du dispositif DataPower.

     Hôte de périphérique
     Dans la zone **Hôte de périphérique**, entrez l'adresse IP du dispositif DataPower surveillé. L'adresse IP par défaut est *9.123.109.139*.

     Port d'interface de gestion XML
     Pour **Port d'interface de gestion XML**, entrez le numéro de port de l'interface de gestion XML. Le numéro par défaut est 5550.

     ID utilisateur
     Pour **ID utilisateur**, entrez l'ID utilisateur de connexion au dispositif DataPower surveillé. La valeur par défaut est admin.

     Mot de passe
     Pour **Mot de passe**, entrez le mot de passe de connexion au dispositif DataPower surveillé, puis confirmez le mot de passe.

     Profil de proxy SSL
     Pour **Profil de proxy SSL**, entrez le chemin d'accès absolu du certificat public de votre profil de proxy SSL si l'interface de gestion XML du périphérique est configurée pour utiliser le profil. Par exemple,

     l'emplacement du fichier .pem exporté à partir des dispositifs Datapower`/mycert.pem`

     où *l'emplacement du fichier .pem exporté à partir des dispositifs Datapower* correspond au chemin d'accès absolu du certificat public. Pour exporter le certificat public, voir Exportation du certificat public.

Option de proxy SSL
Définissez l'**option de proxy SSL** sur `Yes` si l'interface de gestion XML du dispositif surveillé est configurée pour utiliser un profil de proxy SSL personnalisé. Sinon, définissez-la sur `No`.

6. Pour surveiller plusieurs dispositifs DataPower, répétez les étapes 4, à la page 291 et 5, à la page 291 pour configurer une instance d'agent pour chaque dispositif DataPower. Sinon, tapez 5 et appuyez sur **Entrée** pour terminer la configuration.
7. Exécutez la commande suivante pour démarrer l'agent :
   `./datapower-agent.sh start nom_instance`

- Configuration en mode silencieux
  1. Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :
     – Linux AIX Ouvrez *rép_install*`/samples/datapower_silent_config.txt` dans un éditeur de texte.
     – Windows Ouvrez *rép_install*`\samples\datapower_silent_config.txt` dans un éditeur de texte.
  2. Pour configurer l'agent DataPower de sorte qu'il surveille un dispositif, entrez les propriétés suivantes :

     Hôte de périphérique
     Entrez le nom d'hôte ou l'adresse IP du périphérique. Par exemple, **SOAP_HOST.ManageSystemName=** *datapower01*.

     Port d'interface de gestion XML
     Entrez le numéro de port de l'interface de gestion XML. Valeur par défaut : 5550. Par exemple, **DP_PORT.ManageSystemName=** *5550*.

     ID utilisateur
     Entrez l'ID utilisateur de connexion au périphérique. La valeur par défaut est admin. Par exemple, **DP_UID.ManageSystemName=** *admin*.

     Mot de passe
     Entrez le mot de passe de l'ID utilisateur. Par exemple, **DP_PASSWORD.ManageSystemName=** *mot de passe*.

     Profil de proxy SSL
     Entrez le chemin d'accès absolu du certificat public de votre profil de proxy SSL si l'interface de gestion XML du périphérique est configurée pour utiliser le profil. Par exemple,
     l'emplacement du fichier .pem exporté à partir des dispositifs Datapower`/mycert.pem`

     où *l'emplacement du fichier .pem exporté à partir des dispositifs Datapower* correspond au chemin d'accès absolu du certificat public. Pour exporter le certificat public, voir Exportation du certificat public.

     Option de proxy SSL
     Définissez l'**option de proxy SSL** sur `Yes` si l'interface de gestion XML du dispositif surveillé est configurée pour utiliser un profil de proxy SSL personnalisé. Sinon, configurez-la sur `No`. Par exemple : **DP_SSL_OPTION.ManageSystemName1=** `Yes`.

     Important : `ManageSystemName` est unique. Vous devez le remplacer par votre propre nom de système dans toutes les entrées. Pour surveiller plusieurs dispositifs, copiez et répétez les étapes affichées pour surveiller un dispositif. Veillez à définir les paramètres appropriés pour les dispositifs `ManageSystemName` et DataPower.
  3. Accédez au répertoire d'installation de l'agent et exécutez la commande suivante pour démarrer l'agent :
     `./datapower-agent.sh start nom_instance`

Que faire ensuite

- Pour vérifier les noms et les paramètres des instances d'agent configurées, lancez la commande **./cinfo -s bn**.
- Vous pouvez vérifier que les données de l'agent DataPower sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.
- Pour afficher les données de suivi des transactions dans la console Cloud APM, configurez le suivi des transactions pour l'agent DataPower. Pour plus d'informations, voir Configuration du suivi des transactions pour l'agent DataPower.
- Pour afficher la surveillance à différents niveaux, configurez le dispositif DataPower en conséquence. Pour les instructions, voir Surveillance des ressources, Suivi des transactions de middleware et Suivi des transactions de niveau instance des dispositifs DataPower.

Configuration du suivi des transactions pour l'agent DataPower

Pour afficher les données de suivi des transactions pour les dispositifs DataPower dans les tableaux de bord de topologie et du middleware, vous devez activer le suivi des transactions pour l'agent DataPower.

Avant de commencer

- Installez l'agent DataPower et configurez-le pour qu'il se connecte au dispositif DataPower.
- Activez la surveillance pour SOAP ou ARM sur le dispositif DataPower.

Procédure

Pour activer le suivi des transactions pour l'agent DataPower, procédez comme suit :

1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**.
2. Dans l'onglet **DataPower**, sélectionnez les instances d'agent pour lesquelles vous voulez activer le suivi des transactions.
3. Sélectionnez **Actions** > **Set Transaction Tracking** > **Enabled** pour activer le suivi des transactions. Le statut de l'agent dans la colonne **Transaction Tracking** est mis à jour sur **Enabled**.

Résultats

Vous venez d'activer le suivi des transactions pour les instances d'agent sélectionnées.

Que faire ensuite

Pour afficher les données d'un dispositif DataPower dans les tableaux de bord du middleware et de la topologie, vous devez à présent ajouter les dispositifs à surveiller au tableau de bord d'Application Performance. Pour plus d'informations sur l'ajout d'un dispositif DataPower au Tableau de bord d'Application Performance, voir «Ajout d'applications middleware au Tableau de bord d'Application Performance», à la page 107.

Remarque : Si vous utilisez Integration Services et souhaitez surveiller les données transmises entre IBM Integration Bus et DataPower, des étapes de configuration supplémentaires sont requises pour pouvoir afficher un widget Agréger une topologie de transaction exact. L'agent IBM Integration Bus ne peut pas inclure la prise en charge de la corrélation pour les messages SOAP sans enveloppe SOAP. Les noeuds `SOAPRequest`, `SOAPAsyncRequest` et `SOAPReply` peuvent accepter des messages sans enveloppe SOAP sous la forme de messages d'entrée. Pour ces noeuds, la vue de topologie n'affiche aucune relation de la médiation vers la médiation aval ou le serveur d'applications. Pour éviter ce problème, insérez un noeud `SOAPEnvelope` immédiatement avant les noeuds `SOAPRequest`, `SOAPAsyncRequest` ou `SOAPReply` dans votre flux de messages IBM Integration Bus et sélectionnez l'option **Create new envelope** pour le noeud `SOAPEnvelope` pour ajouter une enveloppe SOAP pour le message SOAP.

Configuration de la surveillance de Db2

L'Monitoring Agent for Db2 surveille la disponibilité et les performances du serveur Db2. Vous pouvez surveiller plusieurs serveurs à partir de la console Cloud APM ; chaque serveur est surveillé par une instance Agent Db2. La surveillance à distance est également prise en charge par l'Agent Db2.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Db2.

Pourquoi et quand exécuter cette tâche

L'Agent Db2 est un agent à instances multiples. Vous devez commencer par créer l'instance, puis démarrer l'agent manuellement.

Le nom de système géré inclut le nom d'instance d'agent que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Le nom d'instance d'agent doit être celui de l'instance Db2 actuellement surveillée. Le nom de système géré admet jusqu'à 32 caractères. Le nom d'instance d'agent que vous entrez admet jusqu'à 8 caractères, sans compter la longueur de votre nom d'hôte. Par exemple, si vous indiquez `DB2inst1` comme nom d'instance d'agent, le nom du système géré est `DB2inst1:hostname:ud`.

Important : Si vous indiquez un nom d'instance d'agent long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas complètement.

Afin d'éviter tout problème de droits lorsque vous configurez l'agent, veillez à utiliser le même ID d'utilisateur superutilisateur ou non superutilisateur que celui utilisé pour installer l'agent. Si vous avez installé votre agent en tant qu'un utilisateur sélectionné et que vous souhaitez configurer l'agent en tant qu'un autre utilisateur, consultez «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 219. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez le démarrer en tant qu'un autre utilisateur, voir «Démarrage d'agents en tant qu'utilisateur non superutilisateur», à la page 1039.

Exécutez le script de configuration pour créer une instance et changer les paramètres de configuration. Vous pouvez éditer le fichier de réponses silencieux Db2 avant d'exécuter le script de configuration afin d'éviter l'affichage des invites et la saisie des réponses qui sont normalement nécessaires.

Après avoir configuré l'Agent Db2, veillez à démarrer l'agent avec un ID utilisateur doté du droit Db2 SYSADM sur l'instance surveillée. L'agent doit disposer des droits SYSADM pour activer tous les inverseurs logiques du moniteur. Par conséquent, il est nécessaire que l'agent soit démarré par un agent disposant des droits SYSADM. Utilisez l'utilisateur propriétaire de l'instance, qui détient les droits SYSADM, pour démarrer l'agent.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 43. Versions d'agent et documentation

Version de l'Agent Db2	Documentation
07.10.11.00, 07.10.10.00, 07.10.09.00, 07.10.08.00	IBM Performance Management 8.1.4*
07.10.07.00,07.10.06.00	IBM Cloud Application Performance Management
07.10.05.00	IBM Performance Management 8.1.3 *

Tableau 43. Versions d'agent et documentation (suite)

Version de l'Agent Db2	Documentation
07.10.04.00	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Procédure

Pour configurer l'agent avec les paramètres par défaut, procédez comme suit :

1. Exécutez la commande suivante, où *nom_instance* correspond au nom que vous souhaitez attribuer à l'instance :

   ```
   rép_install/bin/db2-agent.sh config nom_instance
    rép_install/samples/db2_silent_config.txt
   ```

2. Exécutez la commande suivante pour démarrer l'Agent Db2 :

   ```
   rép_install/bin/db2-agent.sh start nom_instance
   ```

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 299.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Avant de commencer

Avant de commencer à configurer l'Agent Db2 pour la surveillance en local et à distance, veillez à réaliser la tâche suivante pour la surveillance à distance.

- Configuration de l'environnement client/serveur pour la surveillance à distance ; voir «Prérequis pour la surveillance à distance», à la page 304.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour DB2**, puis cliquez sur **Configuration de l'agent**.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Important : Pour la surveillance en local, le nom de l'instance d'agent doit être celui de l'instance Db2 actuellement surveillée.

   Pour la surveillance à distance, le nom de l'instance d'agent doit être le nom unique du noeud catalogue.
4. Dans la fenêtre Agent de surveillance pour DB2, procédez comme suit :
   a. Dans la zone **Username**, entrez le nom d'utilisateur de l'instance Db2.

      Pour Db2 en local, entrez le nom du propriétaire d'instance Db2.

      Pour Db2 à distance, entrez le nom réel du propriétaire d'instance Db2 sur la machine Db2 distante.

Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.

b. Dans la zone **Password**, entrez le mot de passe de l'instance Db2.

Pour Db2 en local, entrez le mot de passe du propriétaire d'instance Db2.

Pour Db2 à distance, entrez le mot de passe réel du propriétaire d'instance Db2 sur la machine Db2 distante.

Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.

c. Dans la zone **DB2Customized SQL Definition File**, entrez le chemin de fichier complet du fichier de définition SQL. Si le fichier de définition SQL se trouve le répertoire par défaut, laissez cette zone vide. Sinon, entrez le chemin complet du fichier. Le nom de fichier par défaut avec le chemin d'accès est le suivant :

Linux AIX `CANDLEHOME/config/kudcussql.properties`

Windows `CANDLEHOME\TMAITM6_x64\kudcussql.properties`

d. Dans la zone **db2diag Log File Path**, entrez le chemin de répertoire du fichier journal db2diag. Si le fichier journal db2diag se trouve le répertoire par défaut, laissez cette zone vide. Sinon, indiquez le chemin d'accès du répertoire. Le chemin du répertoire par défaut est le suivant :

Linux AIX `/home/`*`rép_base_propriétaireDB2`*`/sqllib/db2dump`

Windows `C:\ProgramData\IBM\DB2\DB2COPY\`*`NOMINSTANCEDB2`*

Remarque : Ce paramètre n'est pas applicable à la surveillance à distance.

e. Dans la zone **MSGID Filter in Regular Expression**, entrez *MSGID* pour filtrer le journal de diagnostic. MSGID est une combinaison du type de message, du numéro de message et du niveau de gravité. Utilisez une expression régulière pour filtrer le journal en fonction du type de message, du numéro de message, ou du niveau de gravité, par exemple, `ADM1\d*1E|ADM222\d2W`.

f. Dans la liste **Enable Monitoring for Partitions in Remote Hosts**, sélectionnez `Yes` pour indiquer que l'Agent Db2 peut surveiller des partitions sur des hôtes distants.

g. Dans la liste **Enable Monitoring All Databases**, sélectionnez `Yes` pour indiquer que l'Agent Db2 peut surveiller toutes les bases de données.

h. Cliquez sur **OK**. L'instance de l'agent est affichée dans la fenêtre IBM Cloud Application Performance Management.

5. Procédez comme suit pour configurer la surveillance à distance.
   a. Ouvrez *`rép_install`*`\TMAITM6_x64\KUDENV_<nom_instance>`.
   b. Définissez *KUD_DB2_CLIENT_INST* sur le nom de l'instance client Db2 sous lequel l'instance du serveur Db2 distante est cataloguée.
6. Cliquez avec le bouton droit de la souris sur l'instance **Agent de surveillance pour DB2**, puis cliquez sur **Démarrer**.

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de l'Agent Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 299.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Linux ou UNIX

Exécutez le script de configuration pour configurer l'agent sur les systèmes Linux.

Avant de commencer

Avant de commencer à configurer l'Agent Db2 pour la surveillance en local et à distance, veillez à réaliser la tâche suivante pour la surveillance à distance.

- Configuration de l'environnement client/serveur pour la surveillance à distance ; voir «Prérequis pour la surveillance à distance», à la page 304.

Procédure

1. Exécutez la commande *rép_install*/bin/db2-agent.sh config *nom_instance*

   Où *nom_instance* est le nom à attribuer à l'instance :

   Important : Pour la surveillance en local, le nom de l'instance d'agent doit être celui de l'instance Db2 actuellement surveillée.

   Pour la surveillance à distance, il s'agit du noeud catalogué local de l'instance du serveur Db2 distante à surveiller.
2. Lorsque vous êtes invité à saisir une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une valeur et appuyez sur Entrée :
   - Username
   - Password
   - DB2 SQL path
   - Diaglog path
   - Diaglog message ID filter
   - Monitor remote partitions
   - Monitor all databases
3. Exécutez la commande suivante pour démarrer l'agent :

   Pour la surveillance en local, exécutez *rép_install*/bin/db2-agent.sh start *nom_instance* en tant que propriétaire de l'instance Db2.

   Pour la surveillance à distance, exécutez *rép_install*/bin/db2-agent.sh start *nom_noeud* en tant que propriétaire de l'instance client Db2 sous lequel l'instance du serveur Db2 distante est cataloguée.

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de l'Agent Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 299.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Utilisez le fichier de réponses silencieux pour configurer l'agent sans répondre aux invites quand vous exécutez le script de configuration. Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent sur les systèmes Windows et Linux.

Avant de commencer

Avant de commencer à configurer l'Agent Db2 pour la surveillance en local et à distance, veillez à réaliser la tâche suivante pour la surveillance à distance.

- Configuration de l'environnement client/serveur pour la surveillance à distance ; voir «Prérequis pour la surveillance à distance», à la page 304.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration. Vous éditez les valeurs de paramètre dans le fichier de réponses, et exécutez le script de configuration pour créer une instance d'agent et mettre à jour les valeurs de configuration.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `db2_silent_config.txt` disponible à l'emplacement suivant :

   Linux AIX *rép_install*`/samples/db2_silent_config.txt`

   Windows *rép_install*`\tmaitm6_x64\samples\db2_silent_config.txt`
2. Dans le fichier de réponses, indiquez une valeur pour les paramètres suivants :
   - Dans la zone **Username**, entrez le nom d'utilisateur de l'instance Db2.

     Pour Db2 en local, entrez le nom du propriétaire d'instance Db2.

     Pour Db2 à distance, entrez le nom réel du propriétaire d'instance Db2 sur la machine Db2 distante.

     Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.
   - Dans la zone **Password**, entrez le mot de passe de l'instance Db2.

     Pour Db2 en local, entrez le mot de passe du propriétaire d'instance Db2.

     Pour Db2 à distance, entrez le mot de passe réel du propriétaire d'instance Db2 sur la machine Db2 distante.

     Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.
   - Pour le paramètre **`DB2 SQL path`**, laissez à blanc cette zone si le fichier de définition SQL est disponible dans le répertoire par défaut. Sinon, entrez le chemin de répertoire correct. Le fichier de définition SQL est disponible au chemin d'accès par défaut suivant :

     Linux AIX `CANDLEHOME/config/kudcussql.properties` Par exemple, **`KUD_DB2_SQL_PATH=`** `/opt/ibm/apm/agent/config/kudcussql.properties`

     Windows `CANDLEHOME\TMAITM6_x64\kudcussql.properties` Par exemple, **`KUD_DB2_SQL_PATH=`** `C:\IBM\ITM\TMAITM6_x64\kudcussql.properties`
   - Pour le paramètre **`dialog path`**, laissez à blanc cette zone si le fichier journal `db2diag` est disponible dans le répertoire par défaut. Sinon, entrez le chemin de répertoire correct. Le fichier journal est disponible au chemin d'accès par défaut suivant :

     Linux AIX `/home/rép_base_propriétaireDB2/sqllib/db2dump`
     Par exemple, **`KUD_DIAGLOG_PATH=`** `/home/db2inst1/sqllib/db2dump`.

     Windows `unité_installation_Windows:\ProgramData\IBM\DB2\DB2COPY\DB2INSTANCENAME`
     Par exemple, **`KUD_DIAGLOG_PATH=`** `C:\ProgramData\IBM\DB2\DB2COPY1\DB2`

     Remarque : Ce paramètre n'est pas applicable à la surveillance à distance.
   - Pour le paramètre **`dialog message ID filter`**, indiquez *MSGID* pour filtrer le journal de diagnostic. MSGID est une combinaison du type de message, du numéro de message et du niveau de gravité. Vous pouvez également utiliser une expression régulière, par exemple **`KUD_DIAGLOG_MSGID_FILTER=`** `ADM1\d*1E|ADM222\d2W`.
   - Pour le paramètre **`monitor remote partitions`**, entrez `Yes` pour indiquer que l'Agent Db2 surveille des partitions sur des hôtes distants. Par exemple, **`KUD_MONITOR_REMOTE_PARTITIONS=`** *Yes*.
   - Pour le paramètre **`monitor all databases`**, entrez `Yes` pour indiquer que vous souhaitez que l'Agent Db2 surveille toutes les bases de données. Par exemple, **`KUD_MONITOR_ALL_DATABASES=`** *Yes*.
3. Sauvegardez et fermez le fichier `db2_silent_config.txt` et exécutez la commande suivante :

Linux AIX *rép_install*/bin/db2-agent.sh config *nom_instance* *rép_install*/samples/db2_silent_config.txt

Windows *rép_install*\bin\db2-agent.bat config*nom_instance* \tmaitm6_x64\samples\db2_silent_config.txt

<*nom_instance*> est

- Pour la surveillance en local du serveur Db2 : le nom de l'instance du serveur Db2 que vous voulez surveiller.
- Pour la surveillance à distance du serveur Db2 : le nom du noeud catalogue de l'instance du serveur Db2 distante.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Pour Windows, ouvrez le fichier CANDLEHOME\TMAITM6_x64\KUDENV_<nom_instance> et éditez la ligne KUD_DB2_CLIENT_INST comme suit : KUD_DB2_CLIENT_INST=<nom de l'instance client sous lequel l'instance du serveur Db2 distant est cataloguée>
5. Exécutez la commande suivante pour démarrer l'agent :

   Linux AIX *rép_install*/bin/db2-agent.sh start *nom_instance*

   Windows *rép_install*\bin\db2-agent.bat start nom_instance

   A faire : Lors de la surveillance de l'instance du serveur Db2 distante sous UNIX ou Linux, la commande doit être exécutée en tant que propriétaire de l'instance client sous lequel l'instance du serveur distant est cataloguée.

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de l'Agent Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2».
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Octroi de privilèges pour l'affichage des mesures Db2

Pour surveiller les ressources Db2, un utilisateur Db2 doit disposer des droits Db2 SYSADM, SYSCTRL, SYSMAINT et SYSMON pour l'instance surveillée afin de visualiser les données pour certains attributs de l'Agent Db2.

Pourquoi et quand exécuter cette tâche

Pour afficher les données de surveillance que l'agent collecte pour tous les attributs du tableau de bord, l'utilisateur Db2 doit disposer de privilèges spécifiques. Pour affecter ces privilèges à l'utilisateur Db2, exécutez le fichier de script qui se trouve à l'emplacement suivant :

Linux AIX *rép_install*/config/KudGrantUserPermissions.sh

Windows *rép_install*\TMAITM6_x64\KudGrantUserPermissions.bat

Un utilisateur Db2 disposant du droit d'accès SYSADM peut exécuter le script permettant d'octroyer des privilèges à lui-même ou à n'importe quel autre utilisateur Db2. Pour une instance Db2, utilisez le propriétaire d'instance, qui dispose déjà du droit d'accès SYSADM, pour exécuter le script qui lui permet d'octroyer d'autres droits à lui-même ou l'ensemble des droits à tout autre utilisateur Db2.

Procédure

1. Pour la surveillance en local, procédez comme suit.
   a. Sur le système où l'Agent Db2 est installé, ouvrez l'interface de ligne de commande Db2.
   b. Exécutez la commande suivante, où *nom_instance* est le nom de l'instance Db2 et *nom_utilisateur* est le nom de l'utilisateur Db2 :

      Linux AIX *rép_install*/config/KudGrantUserPermissions.sh *nom_instance nom_utilisateur*

      Windows *rép_install*\TMAITM6_x64\KudGrantUserPermissions.bat *nom_instance nom_utilisateur*

      Remarque : Pour les systèmes Windows, *nom_utilisateur* est facultatif dans la commande. Si aucun nom d'utilisateur n'est spécifié dans la commande, les privilèges sont affectés à l'utilisateur par défaut (système).
2. Pour la surveillance à distance, procédez comme suit.
   a. Copiez le fichier KudGrantUserPermissions.sh pour Unix ou Linux et le fichier KudGrantUserPermissions.bat pour Windows, figurant dans le répertoire *rép_install*/TMAITM6_x64/ du poste de travail d'agent, sur la machine du serveur Db2.
   b. Exécutez la commande suivante en tant que propriétaire de l'instance Db2, où *nom_instance* est le nom de l'instance Db2 et *nom_utilisateur* est le nom de l'utilisateur Db2 :

      Linux AIX ./KudGrantUserPermissions.sh *nom_instance nom_utilisateur*

      Windows KudGrantUserPermissions.bat *nom_instance nom_utilisateur*

      A faire : Pour la surveillance à distance de Db2 sous Windows, *nom_utilisateur* doit correspondre au nom d'utilisateur fourni pendant la configuration de l'Agent Db2 sur le poste de travail client.

Configuration des variables d'environnement local

Vous pouvez configurer les variables d'environnement local pour modifier le comportement de Agent Db2.

Procédure

1. Sur les systèmes Windows, cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Advanced > Edit ENV File**.
3. Sur les systèmes Linux ou AIX, accédez à la ligne de commande et éditez le fichier ud.environment à partir du répertoire rép_install/config, rép_install représentant le répertoire d'installation de l'agent.

   Remarque : Le fichier ud.environment est un fichier caché.
4. Dans le fichier des variables d'environnement, entrez des valeurs pour les variables d'environnement.

   Pour plus d'informations sur les variables d'environnement que vous pouvez configurer, voir «Variables d'environnement local».

Variables d'environnement local

Vous pouvez changer le comportement de Agent Db2 en définissant les variables d'environnement local.

Variables permettant de définir la méthode de collecte des données pour le jeu de données de l'espace table

Pour définir la méthode de collecte de données pour le jeu de données de l'espace table, utilisez les variables d'environnement suivantes :

- **KUD_T1_BY_SQL** : utilisez cette variable pour définir la méthode de collecte de données pour le jeu de données de l'espace table à l'aide de requêtes SQL. Pour activer la collecte de données à l'aide de requêtes SQL, définissez la valeur de cette variable sur Y. Pour collecter des données pour le jeu de données de l'espace table à l'aide de la méthode d'image instantanée, définissez la valeur de cette variable sur N. La valeur par défaut de cette variable est N.

  Important : Pour collecter des données à l'aide de requêtes SQL, la version de Db2 doit être 9.7 ou supérieure. En outre, l'utilisateur qui démarre l'Agent Db2 doit disposer du droit d'accès SYSADM pour l'ensemble des bases de données.
- **KUD_T1_DISABLE** : utilisez cette variable pour désactiver la collecte de données pour le jeu de données de l'espace table. Pour activer la collecte de données pour le jeu de données de l'espace table, définissez la valeur de cette variable sur N. Pour désactiver la collecte de données pour le jeu de données de l'espace table, définissez la valeur de cette variable sur Y. La valeur par défaut de cette variable est N.

Variable permettant d'exclure les noeuds CF (Caching Facility) de la collection de données

Pour exclure les noeuds CF (Caching Facility) de l'algorithme de collecte de données dans l'environnement pureScale, utilisez la variable **DB2_CF_PARTITION_NUMS**. Dans le fichier d'environnement de l'agent, définissez la variable **DB2_CF_PARTITION_NUMS** sur DB2_CF_PARTITION_NUMS=<nombre de noeuds CF>. Par exemple, DB2_CF_PARTITION_NUMS=1. Pour plusieurs noeuds CF, spécifiez pour la variable **DB2_CF_PARTITION_NUMS** une liste qui utilise l'un des caractères spéciaux # . : , ; | @ comme délimiteur. Par exemple, DB2_CF_PARTITION_NUMS=12,13,23,34. Aucune valeur par défaut n'est définie pour cette variable.

Variable permettant de limiter la collecte de données pour le jeu de données de tables Db2

Pour définir le nombre maximal de lignes que l'Agent Db2 doit renvoyer, tout en collectant des données pour le jeu de données de tables Db2, utilisez la variable d'environnement **KUD_TABLE_NUMBER**. La valeur par défaut est 10000.

Variable permettant de définir l'intervalle de rechargement du fichier de propriétés SQL personnalisé

Pour définir l'intervalle de temps de rechargement (en secondes) pour le fichier de propriétés SQL personnalisé, utilisez la variable **KUD_CUS_SQL_INTERVAL**. La valeur par défaut est 20 secondes.

Variable permettant de limiter les lignes dans la collecte de données pour le jeu de données Evénement de l'agent

Pour définir le nombre de lignes pour la collecte de données du jeu de données Evénement de l'agent, utilisez la variable **KUD_AGENT_EVENT_CACHE**. Le jeu de données Evénement de l'agent fournit des informations détaillées sur les événements prédéfinis et déclenchés et détermine les problèmes de santé de la base de données surveillée. La valeur par défaut est 50.

Variable permettant de limiter les lignes dans la collecte de données pour le jeu de données Enregistrement du journal Db2

Pour définir le nombre de lignes pour la collecte de données du jeu de données Enregistrement du journal Db2, utilisez la variable **KUD_DBHISTORY_MAXROW**. Le jeu de données Enregistrement du journal Db2 fournit des informations historiques sur le journal d'archivage de Db2. La valeur par défaut est 500.

Variables permettant de définir la collecte des données pour le jeu de données Journal de diagnostic Db2

Pour définir la méthode de collecte de données pour le jeu de données Journal de diagnostic Db2, utilisez les variables d'environnement suivantes :

- **KUD_DIAGLOG_BY_TABLE** : utilisez cette variable pour définir la méthode de collecte de données pour le jeu de données Journal de diagnostic Db2. Si la valeur de cette variable est définie sur Y, alors les données pour le jeu de données Journal de diagnostic Db2 sont collectées à l'aide des requêtes SQL. Si la valeur de cette variable est définie sur N, alors les données pour le jeu de données Journal de diagnostic Db2 sont collectées par analyse du fichier `db2diag.log`. La valeur par défaut de cette variable est `Y`.

  Important : Pour collecter des données à l'aide de requêtes SQL, la version de Db2 doit être 10 ou supérieure.
- **KUD_DIAGLOG_TAILCOUNT** : utilisez cette variable pour définir le nombre de lignes du fichier `db2diag.log` que l'Agent Db2 analyse pour collecter des données pour le jeu de données Journal de diagnostic DB2. Cette variable limite le traitement du fichier journal par l'Agent Db2 de façon à ce que seuls les événements et les messages les plus récents soient surveillés. La valeur par défaut de cette variable est `1000`.
- **KUD_DIAGLOG_CACHE** : utilisez cette variable pour limiter le nombre d'enregistrements de journal qui s'affichent sur le tableau de bord pour le jeu de données Journal de diagnostic Db2. La valeur par défaut de cette variable est `20`.
- **KUD_DIAGLOG_INTERVAL** : utilisez cette variable pour définir l'intervalle de temps de rechargement (en secondes) du fichier `db2diag.log` pour collecter des données pour le jeu de données Journal de diagnostic Db2. La valeur par défaut de cette variable est `30 secondes`.
- **KUD_DISABLE_DIAGLOG** : utilisez cette variable pour désactiver la collecte de données pour le jeu de données Journal de diagnostic Db2. Pour activer la collecte de données pour le jeu de données Journal de diagnostic Db2, définissez la valeur de cette variable sur N. Pour désactiver la collecte de données pour le jeu de données Journal de diagnostic Db2, définissez la valeur de cette variable sur Y. La valeur par défaut de cette variable est `N`.

Variable de définition du délai d'expiration de la requête

Si une requête SQL prend très longtemps pour s'exécuter, cela affecte les performances de l'Agent Db2. Pour définir le délai d'expiration de requête pour l'Agent Db2, utilisez la variable **KUD_QUERY_TIMEOUT**. Cette variable d'environnement permet de définir le délai maximal (en secondes) pendant lequel l'Agent Db2 attend une réponse pour une requête envoyée au serveur Db2. La valeur par défaut de cette variable doit être inférieure à `300` secondes. La valeur par défaut de cette variable est `45 secondes`.

Variable permettant de définir la collecte des données pour le jeu de données DB2 Database01 (obsolète)

L'agent ne doit pas déclencher de requêtes ASN pour collecter des données pour le jeu de données DB2 Database01 (obsolète) lorsque les schémas ASN ne sont pas présents. Pour activer l'exécution des requêtes ASN, utilisez la variable **KUD_REPLICATION_ON**. Si la valeur de cette variable est définie sur Y, l'Agent Db2 exécute les requêtes ASN même lorsque les schémas ASN ne sont pas présents. Si la valeur de cette variable est définie sur N, l'Agent Db2 n'exécute pas les requêtes ASN. La valeur par défaut de cette variable est `Y`.

Variable permettant de configurer les inverseurs logiques du moniteur lors de la collecte de données à l'aide de la méthode d'image instantanée

Si vous voulez collecter les données de surveillance de l'Agent Db2 à l'aide de la méthode d'image instantanée, activez l'inverseur logique du moniteur Db2 pour le jeu de données. Pour activer l'inverseur logique du moniteur Db2, utilisez la variable **KUD_MON_SWITCH_OVERRIDE**. La liste des inverseurs logiques du moniteur Db2 est la suivante :

LOCK Informations sur les verrous

SORT Informations sur les tris

STATEMENT
Informations sur les instructions SQL

TABLE
Informations sur les activités de table

TIMESTAMP
Informations sur les horodatages

UOW Informations sur les unités d'oeuvre.

Si la valeur de cette variable est définie sur Y, l'Agent Db2 maintient les paramètres de configuration des inverseurs logiques du moniteur Db2. Si la valeur de cette variable est définie sur N, l'Agent Db2 active tous les inverseurs logiques du moniteur pour collecter des données. La valeur par défaut de cette variable est `N`.

Variable permettant de tracer les données en mémoire tampon d'image instantanée Db2 d'un jeu de données

Pour afficher les données collectées pour un jeu de données à l'aide de la méthode d'image instantanée, utilisez la variable **KUD_SNAPSHOT_DUMPOUT**. Si la valeur de cette variable est définie sur Y, l'Agent Db2 vide les données en mémoire tampon d'image instantanée pour les groupes d'attributs dans le fichier journal de l'agent. Si la valeur de cette variable est définie sur N, l'Agent Db2 ne vide pas les données en mémoire tampon d'image instantanée dans le fichier journal de l'agent. La valeur par défaut de cette variable est `N`.

Variable permettant de tracer l'Agent Db2 à l'aide des données en mémoire tampon d'image instantanée d'un jeu de données

Pour tracer l'Agent Db2 à l'aide des données en mémoire tampon d'image instantanée collectées pour un jeu de données, utilisez la variable **KUD_SNAPSHOT_READIN**. Pour activer le traçage d'un Agent Db2, définissez la valeur de cette variable sur Y. Pour désactiver le traçage d'un Agent Db2, définissez la valeur de cette variable sur N.

Variable permettant de définir la méthode de collecte des données pour le jeu de données Conflit de verrouillage

Pour définir la méthode de collecte de données pour le jeu de données Conflit de verrouillage, utilisez la variable **KUD_LOCKCONFLICT_BY_SQL**. Pour collecter des données pour le jeu de données Conflit de verrouillage à l'aide de requêtes SQL, définissez la valeur de cette variable sur Y. Pour collecter des données pour le jeu de données Conflit de verrouillage à l'aide de la méthode d'image instantanée, définissez la valeur de cette variable sur N. La valeur par défaut de cette variable est `Y`.

Important : Pour collecter des données à l'aide de requêtes SQL, la version de Db2 doit être 9.7 FP1 ou supérieure. En outre, l'utilisateur qui démarre l'Agent Db2 doit disposer du droit d'accès SYSADM pour l'ensemble des bases de données.

Variable permettant de surveiller le serveur Db2 distant sous Windows

KUD_DB2_CLIENT_INST : définissez cette variable sur le nom de l'instance client Db2 sous lequel l'instance distante du serveur Db2 est cataloguée. Vous ne devez définir cette variable que si vous utilisez la surveillance à distance où l'agent réside sous Windows.

Prérequis pour la surveillance à distance

Vous pouvez utiliser l'Monitoring Agent for Db2 pour la surveillance à distance. Consultez la rubrique relative aux prérequis pour la surveillance à distance de Db2.

Pourquoi et quand exécuter cette tâche

Pour la surveillance à distance de Db2, vous devez commencer par la configuration de base de l'environnement client/serveur Db2. Effectuez cette configuration pour Windows et UNIX ou Linux.

L'utilisateur doit disposer des droits Db2 SYSADM ou SYSCTRL.

A faire : Suivez toutes les étapes sur le poste de travail de l'agent, à l'exception de l'étape 2.

Procédure

1. Sur le poste de travail de l'Agent Db2, installez le client Db2. La version de ce client doit être supérieure ou égale à la version de l'instance du serveur Db2 à surveiller.
2. Vérifiez que le protocole de communication de l'instance Db2 est TCPIP.
   a. Pour ce faire, exécutez la commande **db2set** sur la ligne de commande Db2.
   b. Si le protocole n'est pas défini sur TCPIP, exécutez **db2set DB2COMM=tcpip** sur la ligne de commande Db2.

   Important : Cette étape est réalisée côté serveur.
3. Cataloguez l'instance du serveur distant au niveau du poste de travail de l'agent Db2 en exécutant la commande suivante.

   Important : L'instance du serveur doit être cataloguée sous l'instance client. Vous devez donc exécuter la commande suivante sur l'instance client.

   db2=>CATALOG TCPIP NODE<nom_noeud> REMOTE <nomhôte/adresse_IP> SERVER <nom_service/numéro_port>

   sur Db2, où :

   a. <*nom_noeud*> représente un pseudonyme local de l'instance Db2 sur le composant client.

      Remarque : Pour UNIX ou Linux, <*nom_noeud*> doit être différent de celui de n'importe quel nom d'instance client Db2 ou serveur Db2 disponible sur le même poste de travail.
   b. <nomhôte/adresse_IP> représente le nom ou l'adresse IP du poste de travail du serveur Db2.
   c. <nom_service/numéro_port> représente le nom de service ou le numéro de port de configuration du protocole TCPIP Db2.

   Pour cataloguer l'instance de serveur Db2 qui s'exécute sur le numéro de port 50000 sur le serveur distant «**myserver**» en tant que noeud «db2node», entrez la commande suivante à partir d'une ligne de commande Db2 :

   db2 => CATALOG TCPIP NODE db2node REMOTE myserver SERVER 50000

   Pour plus de détails sur le noeud catalogue, voir https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.client.doc/doc/t0005621.html
4. Si le poste de travail de l'Agent Db2 s'exécute sous UNIX/Linux,
   - Créez un utilisateur dont le nom de noeud est utilisé dans la commande de catalogage.

Exécutez la commande suivante :

useradd -g <groupe> -m -d <rép_base> <utilisateur> -p <mot_de_passe> où

- **<groupe>** représente un groupe pour les propriétaires d'instance DB2 UDB.
- **<utilisateur>** représente un **nom d'utilisateur** local sur le poste de travail client. Le **nom d'utilisateur** doit être identique au nom du noeud avec lequel l'instance du serveur a été cataloguée sur la machine agent.

- Vérifiez le nom de l'instance client Db2 sous lequel l'instance du serveur Db2 distante est catalogué et attribuez les droits en lecture, écriture et exécution du répertoire de base de l'utilisateur que vous venez de créer au propriétaire de cette instance. Cette étape est nécessaire pour rendre l'environnement client Db2 disponible pour effectuer les opérations sur le noeud distant.
- Exécutez la commande suivante :

  chmod -R 775 /home/<nom_noeud>

  où

  - **<nom_noeud>** représente un nom d'utilisateur local de l'instance Db2 sur le composant client.

5. Cataloguez toutes les bases de données que vous voulez surveiller sur l'instance client figurant sur le poste de travail de l'Agent Db2. Exécutez la commande dans l'interpréteur de commandes Db2 pour cataloguer la base de données.

   CATALOG DATABASE <nom_bdd> AS <alias_bdd> AT NODE <nom_noeud>authentication server

   a. <nom_bdd> représente le nom de la base de données du serveur.
   b. <alias_bdd> représente le pseudonyme local de la base de données sur le client Db2.
   c. <nom_noeud> représente un pseudonyme local de l'instance Db2 sur le composant client où la base de données est cataloguée.

   Pour cataloguer une base de données nommée «sample» sur le noeud catalogue «db2node» portant l'alias «dbAlias1», entrez la commande suivante à partir d'une invite Db2.

   db2 => CATALOG DATABASE sample AS dbAlias1 AT NODE db2node authentication server

Configuration de la surveillance de Hadoop

Vous devez configurer l'Monitoring Agent for Hadoop pour qu'il puisse collecter les données d'un cluster Hadoop surveillé. L'agent peut surveiller un cluster Hadoop à noeud unique et à plusieurs noeuds.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Hadoop.

Assurez-vous que les hôtes suivants peuvent être résolus à partir de l'ordinateur sur lequel l'agent Hadoop est installé :

- Tous les hôtes Hadoop que vous voulez configurer, comme NameNode, ResourceManager, et ainsi de suite
- Hôtes Hadoop ayant seulement le rôle NodeManager

Par exemple, vous pouvez effectuer les étapes suivantes pour résoudre les hôtes :

- Ajoutez l'adresse IP, le nom d'hôte et le nom de domaine complet de tous les hôtes Hadoop au fichier `hosts` qui est disponible à l'emplacement suivant :
  - Windows `C:\Windows\System32\drivers\etc\hosts`
  - Linux AIX `/etc/hosts`
- Ajoutez l'ordinateur sur lequel l'agent Hadoop est installé dans le même domaine que celui des hôtes Hadoop.

A faire : Pour surveiller un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO, vérifiez que tous les hôtes peuvent être résolus à partir de l'ordinateur sur lequel l'agent Hadoop est installé.

Pourquoi et quand exécuter cette tâche

L'agent Hadoop est un agent à instance unique. Une fois l'agent installé, vous devez le configurer manuellement. L'agent Hadoop peut être configuré sur des systèmes Windows, Linux et AIX.

A faire :

- Pour un cluster Hadoop à noeud unique, le même noeud joue tous les rôles, tels que NameNode, ResourceManager et le rôle NameNode secondaire, en fonction de la configuration du cluster Hadoop. Pour un cluster Hadoop à plusieurs noeuds, ce sont d'autres noeuds Hadoop qui jouent ces rôles.
- Lorsque vous configurez l'agent, ce dernier détecte automatiquement les rôles DataNodes et NodeManagers dans le cluster Hadoop actuellement surveillé.

Lorsque vous effectuez une mise à niveau à partir de l'agent qui utilise des sockets (8.1.2 Fix Pack 2, ou version antérieure) vers l'agent qui utilise l'API (8.1.3, ou version supérieure), effectuez les étapes de configuration indiquées dans les rubriques suivantes. Cependant, assurez-vous d'indiquer les noms d'hôte conformément aux instructions suivantes lorsque vous configurez l'agent.

- Le nom de hôte de divers processus démon (NameNode, ResourceManger, etc.) que vous indiquez doit être identique (casse et mise en forme) que les noms de hôte qui sont configurés pour l'agent qui utilise les sockets.
- Le nom de domaine complet doit être utilisé lorsque vous spécifiez un nom d'hôte. Par exemple, `hos1.ibm.com`. Si la longueur du nom de domaine complet dépasse 25 caractères, indiquez seulement le nom d'hôte abrégé sans le nom de domaine. Par exemple, si le nom de domaine complet d'un hôte est *myhadoopclustersetupnode.ibm.com*, le nom d'hôte abrégé est `myhadoopclustersetupnode`.

Une fois que vous avez configuré l'agent mis à niveau et que vous visualisez des données dans la console Cloud APM, annulez les modifications qui ont été apportées dans le fichier `hadoop-metrics2.properties` pour l'agent Hadoop. Pour plus d'informations, voir «Mise à niveau de vos agents», à la page 975.

Sur les systèmes Windows, vous pouvez exécuter l'agent Hadoop en tant qu'utilisateur non-administrateur. Un tel utilisateur nécessite toutefois un droit spécifique pour afficher les données dans les tableaux de bord. Pour plus d'informations sur l'attribution de ce droit, voir «Attribution de droits aux utilisateurs non administrateurs», à la page 313.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 44. Versions d'agent et documentation

Version de l'agent Hadoop	Documentation
8.1.3	IBM Cloud Application Performance Management
8.1.2.2 et 8.1.2.1	IBM Performance Management 8.1.3 *

* Le lien ouvre une rubrique Knowledge Center sur site.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes Windows à l'aide de la fenêtre IBM Performance Management.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour Hadoop**.
3. Cliquez sur **Configuration de l'agent**.

   Avertissement : Si **Configuration de l'agent** est désactivé, cliquez sur **Reconfigurer**.
   La fenêtre **Configure Monitoring Agent for Hadoop** s'ouvre.
4. Pour surveiller le cluster Hadoop avec l'authentification basée sur Kerberos SPNEGO activée, procédez comme suit :
   a. Sous **L'authentification basée sur Kerberos SPNEGO pour les services Hadoop basés sur HTTP dans le cluster Hadoop est-elle activée**, cliquez sur **Oui**. Si vous ne disposez pas de l'authentification basée sur Kerberos SPNEGO pour sécuriser les noeuds finaux REST des services Hadoop basés sur HTTP dans le cluster Hadoop, cliquez sur **No**. Les valeurs des zones **Realm name**, **KDC Hostname**, **SPNEGO principal name** et **SPNEGO keytab file** peuvent alors rester à blanc.
   b. Dans la zone **Nom de domaine**, entrez le nom du domaine Kerberos utilisé pour créer les principaux des services. Généralement, le nom de domaine (realm) correspond à votre nom de domaine (domain). Par exemple, si votre ordinateur se trouve dans le domaine (domain) `tivoli.ibm.com`, le nom de domaine (realm) Kerberos est `TIVOLI.IBM.COM`. Ce nom est sensible à la casse.
   c. Dans la zone **Nom d'hôte KDC**, entrez le nom de domaine complet de l'hôte KDC (centre de distribution de clés) pour le domaine spécifié. Vous pouvez également indiquer l'adresse IP de l'hôte KDC à la place du nom de domaine complet. Dans le cas d'un centre de distribution de clés Active Directory, le contrôleur de domaine est l'hôte KDC.
   d. Dans la zone **SPNEGO principal name**, entrez le nom du principal Kerberos utilisé pour accéder aux noeuds finaux REST authentifiés par SPNEGO des services HTTP. Le nom est sensible à la casse et il est au format `HTTP/`*`nom_hôte_qualifié_complet@domaine_kerberos`*
   e. Dans la zone **Fichier de clés SPNEGO**, entrez le nom du fichier de clés du service SPNEGO avec son chemin d'accès complet ou cliquez sur **Parcourir** et sélectionnez-le. Le fichier de clés contient les noms des principaux et des clés des services Kerberos. Ce fichier fournit un accès direct aux services Hadoop sans nécessiter de mot de passe pour chaque service. Il peut être placé dans le chemin suivant : `etc/security/keytabs/`
      Vérifiez que le nom de principal et le fichier de clés SPNEGO appartiennent au même hôte. Par exemple, si le nom de principal est *HTTP/abc.ibm.com@IBM.COM*, le fichier de clés utilisé doit appartenir à l'hôte *abc.ibm.com* host.
      Si l'agent est installé sur un ordinateur distant, copiez le fichier de clés ou le principal sur l'ordinateur distant, dans n'importe quel chemin, puis spécifiez ce dernier dans la zone **SPNEGO keytab file**.
   f. Cliquez sur **Suivant**.
5. Pour spécifier les valeurs des paramètres du cluster Hadoop, procédez comme suit :
   a. Dans la zone **Nom d'hôte du NameNode**, entrez le nom d'hôte du noeud où le processus démon pour NameNode est exécuté.
   b. Dans la zone **Port du NameNode**, entrez le numéro de port associé au processus démon pour NameNode. Le numéro de port par défaut est 50070.
   c. Dans la zone **Nom d'hôte du gestionnaire de ressources**, entrez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources est exécuté.
   d. Dans la zone **Port du gestionnaire de ressources**, entrez le numéro de port associé au processus démon pour le gestionnaire de ressources. Le numéro de port par défaut est 8088.
   e. Facultatif : Dans la zone **Nom d'hôte du JobHistoryServer**, entrez le nom d'hôte du noeud où le processus démon du JobHistoryServer est exécuté.

f. Facultatif : Dans la zone **Port du JobHistoryServer**, entrez le numéro de port associé au processus démon du JobHistoryServer. Le numéro de port par défaut est 19888.

g. Facultatif : Dans la zone **Nom d'hôte du NameNode supplémentaire**, entrez le nom d'hôte du noeud où le processus démon pour un Namenode secondaire ou de secours est exécuté.

h. Facultatif : Dans la zone **Port du NameNode supplémentaire**, entrez le numéro de port associé au processus démon pour un Namenode secondaire ou de secours.

A faire : Si le NameNode supplémentaire est un NameNode de secours, le numéro de port par défaut associé au processus démon pour un NameNode de secours est 50070. Si le NameNode supplémentaire est un NameNode secondaire, le numéro de port par défaut associé au processus démon pour un NameNode secondaire est 50090.

i. Cliquez sur **Tester la connexion** pour vérifier la connexion aux noms d'hôte et aux ports spécifiés. Une fois que vous avez cliqué sur **Tester la connexion**, un message de validation approprié s'affiche lorsque :

- La connexion aux noms d'hôte et aux ports spécifiés est établie ou a échoué.
- Une valeur pour un nom d'hôte est restée vide.
- Une valeur pour un port est restée vide.
- Une valeur non entière est spécifiée pour un numéro de port.

Mettez à jour les valeurs de configuration comme suggéré dans les messages de validation et vérifiez de nouveau la connexion.

j. Facultatif : Pour ajouter des gestionnaires de ressources de secours dans le cluster Hadoop, cliquez sur **Oui** sous **Gestionnaire(s) de ressource de secours dans le cluster Hadoop**. Vous êtes invité à ajouter les détails relatifs aux gestionnaires de ressources de secours ultérieurement.

k. Facultatif : Pour surveiller les services Hadoop dans le cluster Hadoop géré par Apache Ambari, cliquez sur **Oui** sous **Surveillance des services Hadoop pour les installations Hadoop basées sur Ambari**, puis sur **Suivant**.

6. Facultatif : Pour spécifier les détails du serveur Ambari pour la surveillance des services Hadoop, procédez comme suit :
   a. Dans la zone **Nom d'hôte du serveur Ambari**, entrez le nom de l'hôte sur lequel s'exécute le serveur Ambari.
   b. Dans la zone **Port serveur Ambari**, entrez le numéro de port associé au serveur Ambari. Le numéro de port par défaut est 8080.
   c. Dans la zone **Nom de l'utilisateur Ambari**, entrez le nom de l'utilisateur Ambari.
   d. Dans la zone **Mot de passe de l'utilisateur Ambari**, entrez le mot de passe de l'utilisateur Ambari.
   e. Cliquez sur **Suivant**.
7. Pour spécifier les valeurs des paramètres Java, procédez comme suit :
   a. Dans la liste **Niveau de trace Java**, sélectionnez une valeur pour le niveau de trace utilisé par les fournisseurs Java.
   b. Facultatif : Dans la zone **Arguments JVM**, spécifiez une liste d'arguments pour la machine virtuelle Java. La liste d'arguments doit être compatible avec la version de Java installée avec l'agent.
   c. Cliquez sur **Suivant**.
8. Facultatif : Pour ajouter des gestionnaires de ressources de secours, procédez comme suit :
   a. Cliquez sur **Nouveau**.
   b. Dans la zone **Nom d'hôte du gestionnaire de ressources de secours**, entrez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources de secours est exécuté.
   c. Dans la zone **Port du gestionnaire de ressources de secours**, entrez le numéro de port associé au processus démon pour le gestionnaire de ressources de secours. Le numéro de port par défaut est 8088.

d. Cliquez sur **Tester la connexion** pour valider la connexion au nom d'hôte et au numéro de port spécifiés. Une fois que vous avez cliqué sur **Tester la connexion**, un message de validation approprié s'affiche lorsque :
   - La connexion aux noms d'hôte et aux ports spécifiés est établie ou a échoué.
   - Une valeur pour un nom d'hôte est restée vide.
   - Une valeur pour un port est restée vide.
   - Une valeur non entière est spécifiée pour un numéro de port.

   Mettez à jour les valeurs de configuration comme suggéré dans les messages de validation et vérifiez de nouveau la connexion.

e. Répétez les étapes a, b et c pour ajouter d'autres gestionnaires de ressources de secours. Si vous voulez supprimer un des gestionnaires de ressources de secours, cliquer sur le bouton **Supprimer** correspondant au gestionnaire de ressources de secours que vous voulez supprimer.

f. Cliquez sur **Suivant**.

9. Dans la zone **Chemin d'accès aux classes pour les fichiers JAR**, indiquez le chemin d'accès aux classes des fichiers JAR externes. Ce chemin d'accès aux classes est ajouté au chemin d'accès aux classes généré par l'agent. Vous pouvez laisser cette zone vide.
10. Cliquez sur **OK**. Les paramètres de configuration spécifiés sont sauvegardés.
11. Cliquez avec le bouton droit de la souris sur **Agent de surveillance pour Hadoop**, puis cliquez sur **Démarrer**.

Que faire ensuite

1. Activez les événements de sous-noeud pour visualiser les seuils de génération d'événement de l'agent Hadoop. Pour plus d'informations sur l'activation des événements de sous-noeud, voir «Configuration du tableau de bord pour visualiser des événements Hadoop», à la page 313.
2. Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Linux et AIX

Vous exécutez le script de configuration et répondez aux invites pour configurer l'agent sur les systèmes Linux et AIX.

Procédure

1. Sur la ligne de commande, exécutez la commande suivante : *rép_install*`/bin/hadoop-agent.sh config`
   Où *rép_install* est le répertoire d'installation de l'agent Hadoop. L'agent est installé dans le répertoire d'installation par défaut suivant :
   Linux AIX `/opt/ibm/apm/agent`
2. Quand la ligne de commande affiche le message suivant, entrez 1 pour continuer les étapes de configuration et appuyez sur Entrée.
   ```
   Edit 'Monitoring Agent for Hadoop' setting? [1= yes, 2= No]
   ```
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 pour spécifier les valeurs de surveillance du cluster Hadoop avec l'authentification basée sur Kerberos SPNEGO activée, puis appuyez sur la touche Entrée. Sinon, entrez 2 et appuyez sur Entrée. Vous pouvez conserver une valeur vide pour les zones **Nom de domaine**, **Nom d'hôte KDC**, **Nom du principal SPNEGO** et **Fichier de clés SPNEGO** :
   ```
   Is Kerberos SPNEGO-based authentication for HTTP based Hadoop services in Hadoop cluster
   enabled\: [ 1=Yes, 2=No (default is: 2)
   ```
   a. Pour le paramètre **Nom de domaine**, entrez le nom du domaine Kerberos utilisé pour créer les principaux des services. Généralement, le nom de domaine (realm) correspond à votre nom de

domaine (domain). Par exemple, si votre ordinateur se trouve dans le domaine (domain) `tivoli.ibm.com`, le nom de domaine (realm) Kerberos est `TIVOLI.IBM.COM`. Ce nom est sensible à la casse.

b. Dans la zone **Nom d'hôte KDC**, entrez le nom de domaine complet de l'hôte KDC (centre de distribution de clés) pour le domaine spécifié. Vous pouvez également indiquer l'adresse IP de l'hôte KDC à la place du nom de domaine complet. Dans le cas d'un centre de distribution de clés Active Directory, le contrôleur de domaine est l'hôte KDC.

c. Pour le paramètre **Nom du principal SPNEGO**, entrez le nom du principal Kerberos utilisé pour accéder aux noeuds finals REST authentifiés par SPNEGO des services HTTP. Le nom est sensible à la casse et il est au format `HTTP/`*`nom_hôte_qualifié_complet@domaine_kerberos`*

d. Pour le paramètre **Fichier de clés SPNEGO**, entrez le nom du fichier de clés du service SPNEGO avec son chemin d'accès complet. Le fichier de clés contient les noms des principaux et des clés des services Kerberos. Ce fichier fournit un accès direct aux services Hadoop sans nécessiter de mot de passe pour chaque service. Il peut être placé dans le chemin suivant : `etc/security/keytabs/`
Vérifiez que le nom de principal et le fichier de clés SPNEGO appartiennent au même hôte. Par exemple, si le nom de principal est *HTTP/abc.ibm.com@IBM.COM*, le fichier de clés utilisé doit appartenir à l'hôte *abc.ibm.com* host.
Si l'agent est installé sur un ordinateur distant, copiez le fichier de clés ou le principal sur l'ordinateur distant, dans n'importe quel chemin, puis spécifiez ce dernier pour le paramètre **Fichier de clés SPNEGO**.

4. Lorsque vous êtes invité à entrer les détails du cluster Hadoop, spécifiez une valeur appropriée pour chacun des paramètres suivants, puis appuyez sur Entrée :

a. Pour le paramètre **Nom d'hôte NameNode**, indiquez le nom d'hôte du noeud où le processus démon pour NameNode est exécuté, puis appuyez sur Entrée.

Avertissement : Si vous appuyez sur Entrée sans indiquer de nom d'hôte, vous êtes invité à en entrer un.

b. Pour le paramètre **Port NameNode**, indiquez le numéro de port associé au processus démon pour NameNode, puis appuyez sur Entrée. Le numéro de port par défaut est 50070.

c. Pour le paramètre **Nom d'hôte du gestionnaire de ressources**, indiquez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources est exécuté, puis appuyez sur Entrée.

Avertissement : Si vous appuyez sur Entrée sans indiquer de nom d'hôte, vous êtes invité à en entrer un.

d. Pour le paramètre **Port du gestionnaire de ressources**, indiquez le numéro de port associé au processus démon pour le gestionnaire de ressources. Le numéro de port par défaut est 8088.

5. Facultatif : Lorsque vous êtes invité à ajouter les détails des paramètres suivants du cluster Hadoop, acceptez la valeur par défaut ou spécifiez une valeur appropriée pour chacun des paramètres suivants, puis appuyez sur Entrée :

a. Pour le paramètre **Nom d'hôte du JobHistoryServer**, indiquez le nom d'hôte du noeud où le processus démon pour JobHistoryServer est exécuté.

b. Pour le paramètre **Port du JobHistoryServer**, entrez le numéro de port associé au processus démon pour JobHistoryServer. Le numéro de port par défaut est 19888.

c. Pour le paramètre **Nom d'hôte du NameNode supplémentaire**, indiquez le nom d'hôte du noeud où le processus démon pour un Namenode secondaire ou de secours est exécuté.

d. Pour le paramètre **Port du NameNode supplémentaire**, indiquez le numéro de port associé au processus démon pour un Namenode secondaire ou de secours. Le numéro de port par défaut pour un Namenode secondaire est 50090. Pour un NameNode de secours, le numéro de port par défaut est 50070.

6. Facultatif : Lorsque la ligne de commande affiche le message suivant, entrez 1 pour ajouter les détails des gestionnaires de ressources de secours pour le cluster haute disponibilité, puis appuyez sur Entrée.
`Standby ResourceManager(s) in Hadoop Cluster [ 1=Yes, 2=No ] (default is: 2):`

7. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez ensuite sur la touche Entrée pour surveiller les services Hadoop dans le cluster Hadoop géré par Ambari :
   `Monitoring of Hadoop services for Ambari based Hadoop installations [ 1=Yes, 2=No ] (default is: 2):`
   Sinon, conservez la valeur par défaut 2 et appuyez sur Entrée. Si vous vous activez la surveillance des services Hadoop, spécifiez une valeur pour chacun des paramètres suivants du serveur Ambari, puis appuyez sur Entrée :
   a. Pour le paramètre **Nom d'hôte du serveur Ambari**, entrez le nom de l'hôte sur lequel s'exécute le serveur Ambari.
   b. Pour le paramètre **Port serveur Ambari**, entrez le numéro de port associé au serveur Ambari. Le numéro de port par défaut est 8080.
   c. Pour le paramètre **Nom de l'utilisateur Ambari**, entrez le nom de l'utilisateur Ambari.
   d. Pour le paramètre **Mot de passe de l'utilisateur Ambari**, entrez le mot de passe de l'utilisateur Ambari.
8. Lorsque la ligne de commande affiche le message suivant, sélectionnez le niveau de trace Java approprié et appuyez sur Entrée :
   `This parameter allows you to specify the trace level used by the Java providers Java trace level [ 1=Off, 2=Error, 3=Warning, 4=Information, 5=Minimum Debug, 6=Medium Debug, 7=Maximum Debug, 8=All ] (default is: 2)`
9. Facultatif : Lorsque la ligne de commande affiche le message suivant, spécifiez les arguments pour la machine virtuelle Java et appuyez sur Entrée. La liste d'arguments doit être compatible avec la version de Java installée avec l'agent.
   `This parameter allows you to specify an optional list of arguments to the java virtual machine JVM arguments (default is:)`
10. Facultatif : Lorsque la ligne de commande affiche le message suivant, entrez 1 pour ajouter les détails des gestionnaires de ressources de secours suivants, puis appuyez sur Entrée :
    `Edit 'Hadoop High Availability(HA) Cluster with Standby ResourceManagers' settings, [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5): 1`
    a. Pour le paramètre **`Nom d'hôte du gestionnaire de ressources de secours`**, entrez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources de secours est exécuté.
    b. Pour le paramètre **`Port du gestionnaire de ressources de secours`**, entrez le numéro de port associé au processus démon pour le gestionnaire de ressources de secours. Le numéro de port par défaut est 8088.
    c. Lorsque vous y êtes invité, entrez 1 pour ajouter d'autres gestionnaires de ressources de secours, puis répétez les étapes a et b, ou entrez 5 pour passer à l'étape suivante.
    - Pour éditer les paramètres de configuration d'un gestionnaire de ressources de secours en particulier, tapez 4 et appuyez sur Entrée jusqu'à ce que le nom d'hôte du gestionnaire de ressources de secours nécessaire s'affiche.
    - Pour retirer un gestionnaire de ressources de secours, tapez 3 et appuyez sur Entrée une fois que le nom d'hôte du gestionnaire de ressources de secours que vous voulez retirer est affiché.
11. Lorsque vous y êtes invité, entrez le chemin d'accès aux classes pour les fichiers JAR nécessaires pour le fournisseur de données API Java, puis appuyez sur Entrée. Les valeurs de configuration spécifiées sont sauvegardées et un message de confirmation s'affiche.
12. Exécutez la commande suivante pour démarrer l'agent : *rép_install*`/bin/hadoop-agent.sh start`

Que faire ensuite

1. Activez les événements de sous-noeud pour visualiser les seuils de génération d'événement de l'agent Hadoop. Pour plus d'informations sur l'activation des événements de sous-noeud, voir «Configuration du tableau de bord pour visualiser des événements Hadoop», à la page 313.
2. Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Pour certains paramètres, les valeurs par défaut sont fournies en commentaire. Vous pouvez spécifier des valeurs différentes pour ces paramètres et supprimer les balises de commentaire qui sont placées au début des paramètres.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent Hadoop sur les systèmes Linux, AIX et Windows.

Procédure

1. Ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*\samples\hadoop_silent_config.txt
2. Dans le fichier de réponses, procédez comme suit :
   a. Lorsque vous souhaitez surveiller le cluster Hadoop activé pour l'authentification basée sur Kerberos SPNEGO, spécifiez yes et entrez des valeurs pour les paramètres suivants :
      - HADOOP_REALM_NAME
      - HADOOP_KDC_HOSTNAME
      - HADOOP_PRINCIPAL_NAME
      - HADOOP_SPNEGO_KEYTAB
   b. Entrez des valeurs pour les paramètres suivants des rôles NameNode (NN), ResourceManager (RM) et Job History Server (JHS) :
      - HADOOP_NN_HOSTNAME
      - HADOOP_NN_PORT
      - HADOOP_RM_HOSTNAME
      - HADOOP_RM_PORT
      - HADOOP_JHS_HOSTNAME (facultatif)
      - HADOOP_JHS_PORT (facultatif)
   c. Facultatif : Pour le paramètre **HADOOP_ADDITIONAL_NN_HOSTNAME**, spécifiez le nom d'hôte du NameNode de secours ou secondaire.
   d. Facultatif : Pour le paramètre **HADOOP_ADDITIONAL_NN_PORT**, spécifiez le numéro de port du NameNode de secours ou secondaire.

      A faire : Si le NameNode supplémentaire est un NameNode de secours, le numéro de port par défaut qui est associé au processus démon NameNode de secours est 50070. Si le NameNode supplémentaire est un NameNode secondaire, le numéro de port par défaut qui est associé au processus démon NameNode secondaire est 50090.
   e. Facultatif : Pour le paramètre **Hadoop_SRM**, indiquez Yes pour ajouter des gestionnaires de ressources (ResourceManager) de secours pour un cluster haute disponibilité, et passez à l'étape g.
   f. Facultatif : Pour surveiller les services Hadoop du cluster Hadoop géré par Ambari, entrez les valeurs de chacun des paramètres suivants, puis appuyez sur Entrée :
      - AMBARI_SERVER_HOSTNAME
      - AMBARI_SERVER_PORT
      - USERNAME_OF_AMBARI_USER
      - PASSWORD_OF_AMBARI_USER
   g. Pour le paramètre **JAVA_TRACE_LEVEL**, indiquez le niveau de trace approprié.
   h. Facultatif : Pour le paramètre **JAVA_JVM_ARGS**, indiquez des arguments pour la machine virtuelle Java™.
   i. Facultatif : Ajoutez le nom d'hôte et le numéro de port d'un ResourceManager de secours au format suivant : HADOOP_SRM_PORT.*hadoop_srm_config_sec_1*=8088 Où *hadoop_srm_config_sec_1* est le nom d'hôte du noeud sur lequel le processus démon pour le ResourceManager de secours

s'exécute, et 8088 est le numéro de port par défaut. Pour ajouter des ResourceManagers de secours, ajoutez le nom d'hôte et le numéro de port de chaque ResourceManager supplémentaire sur de nouvelles lignes, au même format.

3. Sauvegardez le fichier de réponses, puis exécutez la commande suivante :

   Linux AIX `rép_install/bin/hadoop-agent.sh config rép_install/samples/hadoop_silent_config.txt`

   Windows `rép_install/bin/hadoop-agent.bat config rép_install/samples/hadoop_silent_config.txt`

4. Démarrez l'agent :

   Linux AIX Exécutez la commande suivante : `rép_install\bin\hadoop-agent.sh start`

   Windows Cliquez avec le bouton droit de la souris sur **Agent de surveillance pour Hadoop**, puis cliquez sur **Start**.

Que faire ensuite

1. Activez les événements de sous-noeud pour visualiser les seuils de génération d'événement de l'agent Hadoop. Pour plus d'informations sur l'activation des événements de sous-noeud, voir «Configuration du tableau de bord pour visualiser des événements Hadoop».
2. Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration du tableau de bord pour visualiser des événements Hadoop

Vous devez configurer le tableau de bord pour activer les événements de sous-noeud de sorte que l'onglet **Événements** puisse afficher des événements Hadoop.

Pourquoi et quand exécuter cette tâche

La valeur par défaut pour **Activer les événements sous-noeud** est "false". Modifiez cette valeur par "true" pour afficher les événements Hadoop.

Procédure

1. Ouvrez la console Cloud APM et accédez à **Configuration système**.
2. Sur la page Configuration avancée, cliquez sur **Intégration d'UI** sous **Catégories de configuration**.
3. Dans la liste **Activer les événements de sous-noeud**, sélectionnez **Vrai**.
4. Cliquez sur **Save**.

Attribution de droits aux utilisateurs non administrateurs

Sur les systèmes Windows, accordez le droit *Debug program* à un utilisateur non administrateur pour l'exécution de l'agent Hadoop. Ce droit est obligatoire pour pouvoir afficher des données dans les tableaux de bord de l'agent Hadoop.

Procédure

Procédez comme suit sur l'ordinateur où l'agent Hadoop est installé :

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration**.
2. Cliquez deux fois sur **Stratégie de sécurité locale**.
3. Dans le panneau Paramètres de sécurité, développez **Stratégies locales** et cliquez sur **Attribution des droits utilisateur**.
4. Cliquez avec le bouton droit de la souris sur **Déboguer les programmes** et sélectionnez **Propriétés**.

5. Cliquez sur **Ajouter un utilisateur ou un groupe** et ajoutez le nom de l'utilisateur non administrateur auquel vous voulez accorder ce droit.
6. Cliquez sur **OK**.

Que faire ensuite

Configurez et exécutez l'agent Hadoop en tant qu'utilisateur non administrateur.

Configuration de la surveillance de HMC Base

L'Monitoring Agent for HMC Base offre la possibilité de surveiller la console HMC (Hardware Management Console). Il surveille la disponibilité et la santé des ressources HMC : UC, mémoire, stockage et réseau. L'agent génère également des rapports sur l'inventaire et la configuration HMC des serveurs Power, des pools d'UC et des partitions logiques. Les utilisations de l'UC par les serveurs Power, les partitions logiques et les pools sont surveillées à l'aide des exemple de données de performances HMC.

Avant de commencer

Avant de configurer l'agent HMC Base, exécutez les tâches suivantes :

- Configurez la connexion SSH entre le système qui exécute l'agent et la console HMC. Pour plus d'informations, voir «Configuration de la connexion SSH», à la page 316.
- Préparez le SDK de la console HMC avant de démarrer la première instance d'agent. Pour plus d'informations, voir «Préparation du kit SDK pour HMC», à la page 317.

Procédure

- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :
  1. Ouvrez le fichier `hmc_base_silent_config.txt` dans un éditeur de texte :
     - AIX *rép_install*`/samples/hmc_base_silent_config.txt`.
  2. Pour **`HMC Hostname`**, vous pouvez spécifier l'adresse IP ou le nom d'hôte.
  3. Pour **`HMC Username`**, vous devez entrer le nom de l'utilisateur de connexion de la console HMC. Par exemple, **`HMC_USERNAME=`** *hscroot*.

     Remarque : Le nom de l'utilisateur de connexion que vous affectez à la console HMC requiert au minimum les droits hscviewer.
  4. Pour **`HMC Password`**, vous devez saisir le mot de passe de l'utilisateur.
  5. Pour **`Maximum Number of Data Provider Log Files:`**, vous devez spécifier le nombre maximal de fichiers journaux de fournisseur de données créés. Par exemple, **`KPH_LOG_FILE_MAX_COUNT=`***10*.
  6. Pour **`Maximum Size in KB of Each Data Provider Log`**, vous devez entrer la taille maximale en kilooctets qu'un fichier journal de fournisseur de données peut atteindre avant qu'un nouveau fichier journal ne soit créé. Par exemple, **`KPH_LOG_FILE_MAX_SIZE=`** *5190*.
  7. Pour **`Level of Detail in Data Provider Log`**, vous devez entrer la quantité de détails que le fournisseur de données inclut dans les fichiers journaux du fournisseur de données. Par exemple, **`KPH_LOG_LEVEL=`***Fine*. Vous devez spécifier l'une des valeurs suivantes :
     - 1= Off
     - 2=Severe
     - 3=Warning
     - 4=Info
     - 5=Fine
     - 6=Finer

– 7=Finest
– 8=All

Important : La valeur par défaut est 4.

8. Sauvegardez et fermez le fichier `hmc_base_silent_config.txt`, puis entrez : `./hmc_base-agent.sh config` *`nom_instance rép_install`*`/samples/hmc_base_silent_config.txt`, *nom_instance* représentant le nom que vous souhaitez affecter à l'instance et *rép_install*, le répertoire d'installation de l'agent HMC Base. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

- AIX Pour configurer l'agent en répondant à des invites, procédez comme suit :
  1. Ouvrez le répertoire *`rép_install`*`/bin`, où *rép_install* est le répertoire d'installation de l'agent HMC Base.
  2. Pour configurer agent HMC Base, exécutez la commande **`./hmc_base-agent.sh config instance_name`**.
  3. Lorsque le système demande de **`modifier les paramètres de l'agent de surveillance pour HMC Base`**, appuyez sur **Entrée**. La valeur par défaut est `Oui`.
  4. Pour entrer les informations de configuration de la console HMC, procédez comme suit :
     a. Lorsque le système vous demande le **`nom d'hôte HMC`**, tapez le nom d'hôte ou l'adresse IP et appuyez sur **Entrée**.
     b. Lorsque le système vous demande le **`nom d'utilisateur HMC`**, entrez le nom de l'utilisateur de connexion associé à la console HMC, puis appuyez sur **Entrée**.
  5. Lorsque vous y êtes invité, saisissez dans **`HMC Password`** le mot de passe de l'utilisateur.
  6. Pour entrer les informations sur le fournisseur de données, procédez comme suit :
     a. Lorsque le système vous demande le **`nombre maximal de fichiers journaux de fournisseur de données`**, entrez-le, puis appuyez sur **Entrée**.

        Le nombre maximal par défaut de fichiers journaux de fournisseur de données est de 10.
     b. Lorsque le système vous demande le **`la taille maximale en kilooctets de chaque journal de fournisseur de données`**, entrez-la, puis appuyez sur **Entrée**.

        la taille maximale par défaut en kilooctets est de 5190.
     c. Lorsque le système vous demande le **`niveau de détail dans le journal de fournisseur de données`**, entrez l'un des niveaux suivants, puis appuyez sur **Entrée** :
        – 1= Off
        – 2=Severe
        – 3=Warning
        – 4=Info
        – 5=Fine
        – 6=Finer
        – 7=Finest
        – 8=All

Que faire ensuite

- Pour démarrer l'agent, entrez : `./hmc_base-agent.sh start` *`NomInstance`*.
- Configurez le serveur de la console HMC selon les instructions de la rubrique «Configuration du serveur de la console HMC pour la surveillance des entrées-sorties virtuelles», à la page 318 pour la surveillance des entrées-sorties virtuelles.
- Activez la surveillance de l'utilisation de l'UC et de la mémoire selon les instructions de la rubrique «Activation de la surveillance de l'utilisation de l'UC et de la mémoire», à la page 318.

Configuration de la connexion SSH

Vous devez installer la connexion SSH entre le système qui exécute l'agent et la console HMC pour que celui-ci collecte des données.

Pourquoi et quand exécuter cette tâche

Le fournisseur de données d'agent collecte des données à partir de la console de gestion en exécutant des commandes CLI via SSH. Par défaut, le fournisseur de données patiente pendant 1 minute pour l'exécution de la commande CLI. Passé ce délai, le fournisseur de données ferme la session SSH dans laquelle la commande CLI est en cours d'exécution, et aucune des données de cette commande n'est disponible dans les ensembles de données de l'agent jusqu'à ce que la commande aboutisse. Le chemin par défaut de la commande SSH est `/usr/bin/ssh`. Si SSH est installé à un autre emplacement, spécifiez le chemin d'accès à l'aide de la variable d'environnement **KPH_SSH_PATH**.

Procédure

Utilisez l'une des méthodes ci-après pour configurer la connexion SSH.

- Utilisez le script `setup_hmc_key.pl` pour configurer la connexion SSH.
  1. Ouvrez une session sur le serveur sur lequel l'agent est installé.
  2. Ouvrez le répertoire `rép_install/aix526/ph/bin`, `rép_install` correspondant au répertoire d'installation de l'agent HMC Base.
  3. Exécutez la commande `perl setup_hmc_key.pl`.
  4. Répondez aux invites et indiquez le nom d'hôte ou l'adresse IP de la console HMC, le nom d'utilisateur de la console HMC (qui doit avoir des droits d'accès équivalents à `hscviewer`) et le mot de passe pour créer la paire de clés.
  5. Après avoir créé la paire de clés, testez la connectivité en exécutant une commande telle que `ssh hscroot@hmchost lshmc -V`. Si SSH se connecte à la console HMC pour la première fois, ajoutez la console HMC au fichier `ssh known_hosts` en répondant `yes` au message suivant :

     ```
     The authenticity of host 'hmchost (3.3.333.333)' can't be established.
     RSA key fingerprint is 4c:b4:26:27:38:f3:ec:58:01:92:26:f9:61:32:bb:4d.
     Are you sure you want to continue connecting (yes/no)? yes

     Warning: Permanently added 'hmchost,3.3.333.333' (RSA) to the list of known hosts.
     ```

     L'agent peut désormais utiliser SSH pour collecter des données à partir de la console HMC.
- Utilisez l'utilitaire `ssh-keygen` pour générer des clés et configurer la connexion SSH.
  1. Ouvrez une session sur le serveur sur lequel l'agent est installé.
  2. Générez des clés publiques et privées, sans paraphrase, à l'aide de l'utilitaire `ssh-keygen`. Par exemple, la commande suivante génère un ensemble de clés publiques et de clés privées :

     ```
     ssh-keygen -t rsa -f /.ssh/id-rsa
     ```

     Appuyez sur Entrée lorsque vous êtes invité à entrer une paraphrase. La clé publique générée est stockée dans le fichier `/.ssh/id-rsa.pub`. La clé privée est stockée dans le fichier `/.ssh/id-rsa`.
  3. Transférez le fichier qui contient la clé publique à l'ordinateur HMC à l'aide d'utilitaires tels que `scp`.
  4. Sur l'ordinateur HMC, ajoutez le fichier de clés publiques à la collection de clés stockées sur la console HMC. Les clés sont sauvegardées dans le fichier `/.ssh/authorized_keys2`.
  5. Ajoutez le nom d'hôte et la clé de la console HMC au fichier `known_hosts`. Ce fichier se trouve dans le répertoire `/.ssh`.
     a. Exécutez la commande `ssh "user"@"hmc_hostname" -i "private_keyfile" date`.
     b. Indiquez `yes` pour placer les clés dans la mémoire cache. Cette commande ajoute l'entrée au fichier `known_hosts` pour les connexions ultérieures.

6. Exécutez la commande `ssh "user"@"hmc_hostname" date`. Si la date est renvoyée sans l'invite de mot de passe, les clés SSH ont été correctement installées.

Préparation du kit SDK pour HMC

Vous devez préparer le kit SDK pour HMC avant de démarrer l'instance d'agent pour la première fois.

Pourquoi et quand exécuter cette tâche

Avant de démarrer votre première instance d'agent, vous devez préparer la version correspondante du kit SDK pour HMC. Une fois la préparation terminée, il n'est pas nécessaire de répéter cette tâche pour une autre instance de l'agent HMC Base que vous créez pour la console HMC au même niveau de version. Pour surveiller une autre version de la console HMC, répétez cette tâche pour préparer à nouveau le kit SDK.

Procédure

A partir du répertoire *agent_dir*/aix526/ph/bin, exécutez l'outil de script **prepareSDK.sh** pour préparer automatiquement le kit SDK de HMC.

- Si le message `SDK is ready for HMC` s'affiche, la préparation est terminée.
- S'il n'apparaît pas, vous pouvez préparer manuellement le kit SDK pour HMC.

Pour HMC version 8.5.0, procédez comme suit :

1. Utilisez un navigateur pour télécharger le kit SDK de HMC directement avec l'URL suivante :

   `https://`*IP_HMC*`:12443/rest/api/web/sdk`

   Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe de `hscroot`. Le nom du fichier SDK est au format `pmc_sdk_*.zip`.
2. . Décompressez ce fichier et accédez au répertoire `IBM HMC REST Web Services SDK Runtime/lib/ibm`.
3. Copiez tous les fichiers `.jar` du dossier `IBM HMC REST Web Services SDK Runtime/lib/ibm` du kit SDK HMC dans le dossier *agent_dir*`/aix526/ph/lib/`*version_HMC*. Si la version de HMC est 8.5.0, *version_HMC* est similaire à `8502`.

Pour HMC 860, procédez comme suit :

1. Utilisez un navigateur pour télécharger le kit SDK de HMC directement avec l'URL suivante :

   `https://`*IP_HMC*`:12443/rest/api/web/sdk`

   Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe de `hscroot`. Le nom du fichier SDK est au format `pmc-rest-sdk*.zip`.
2. Décompressez ce fichier et accédez au répertoire `lib`.
3. Copiez tous les fichiers `pmc*-8.8.6*.jar` du dossier `lib` du kit SDK HMC dans le répertoire *rép_agent*`/aix526/ph/lib/`*version_HMC*. Si la version HMC est 8.6.0, *version_HMC* est similaire à `8602`.

Résultats

Vous avez préparé le kit SDK pour HMC.

Que faire ensuite

Configurez l'agent HMC Base conformément aux instructions fournies dans «Configuration de la surveillance de HMC Base», à la page 314.

Configuration du serveur de la console HMC pour la surveillance des entrées-sorties virtuelles

Avant que l'agent HMC Base puisse surveiller le statut des entrées-sorties virtuelles, vous devez configurer le serveur de la console HMC.

Procédure

Pour configurer le serveur de la console HMC conformément aux prérequis de l'agent HMC Base afin de surveiller les entrées-sorties virtuelles, procédez comme suit.

- Activez la fonction PMC du serveur de la console HMC et des serveurs virtuels d'entrée-sortie.
  1. Connectez-vous au serveur de la console HMC en utilisant le navigateur en mode classique.
     `https://nomhôte_hmc`
  2. Cliquez sur **HMC Management** > **Change Performance Monitoring Settings**. La fenêtre Change Performance Monitoring Settings s'affiche.
  3. Dans la section **Performance Monitoring Data Collection for Manage Servers**, activez la fonction **Collection** pour les serveurs correspondants.
  4. Cliquez sur chaque serveur virtuel d'entrée-sortie pour afficher la fenêtre Partition Properties pour ce serveur.
  5. Dans l'onglet General, vérifiez que la case de l'option **Allow performance information collection** est cochée. Cliquez sur **OK** pour sauvegarder les paramètres.

  Après plusieurs minutes, vous pouvez visualiser le trafic réseau et de stockage des serveurs correspondants sur la page Performance Monitoring.
- Vérifiez que l'utilisateur HMC de l'agent HMC Base possède le privilège correct.
  1. Lorsque vous ajoutez ou éditez l'utilisateur, vérifiez que l'utilisateur possède le rôle **hmcviewer** et que l'option **AllSystemResource** est activée pour cet utilisateur.
  2. Dans la fenêtre User Properties, activez l'option **Allow remote access via the web**.

Activation de la surveillance de l'utilisation de l'UC et de la mémoire

Si la collecte de données d'utilisation d'UC et de mémoire est désactivée, les données d'utilisation d'UC et de mémoire de chaque serveur d'alimentation ne s'affichent pas dans l'interface utilisateur.

Procédure

Utilisez l'une des méthodes suivantes pour activer la surveillance de l'utilisation de l'UC et de la mémoire.

- Activez la surveillance de l'utilisation de l'UC et de la mémoire en exécutant la commande de gestion HMC `chlparutil`.
  `chlparutil -r config -m <nomCEC> -s <taux d'échantillonnage en secondes, toujours 60>`
- Activez la surveillance de l'utilisation de l'UC et de la mémoire sur le serveur de la console HMC.
  1. Connectez-vous au serveur de la console HMC en mode classique.
  2. Cliquez sur le noeud **Servers** dans l'arborescence de navigation.
  3. Sélectionnez le serveur et accédez à **Operations** > **Utilization Data** > **Change the Sample rate**.
  4. Définissez une fréquence d'échantillonnage. La fréquence d'échantillonnage est désactivée par défaut. Vous pouvez définir la fréquence à l'aide de valeurs appropriées, par exemple `30 minutes`.

Configuration de la surveillance de HTTP Server

L'Monitoring Agent for HTTP Server est automatiquement lancé après l'installation. Pour activer la collecte de données, assurez-vous que le serveur HTTP est en cours d'exécution et éditez le fichier de configuration du serveur HTTP de sorte qu'il inclue une référence au fichier de configuration du collecteur de données de l'agent HTTP Server.

Avant de commencer

Deux fichiers font partie de la configuration de l'agent HTTP Server. Pour visualiser des exemples de ces fichiers, voir Exemples. Localisez et consultez les fichiers suivants :

Fichier de configuration du collecteur de données de l'agent HTTP Server

Après avoir installé l'agent HTTP Server, ce dernier découvre le serveur HTTP et génère un fichier de configuration du collecteur de données dans le répertoire *rép_install*/tmp/khu, où *rép_install* est le répertoire d'installation de l'agent HTTP Server.

Si votre environnement contient plusieurs serveurs HTTP, un fichier de configuration d'agent HTTP Server est généré par serveur HTTP.

Le nom du fichier de configuration de l'agent HTTP Server se compose de deux parties au format suivant :

khu.*chemin d'accès complet/nom du fichier de configuration du serveur HTTP*.conf

La première partie du nom du fichier de configuration d'agent est khu, où hu est le code agent du serveur HTTP.
La seconde partie du nom du fichier de configuration d'agent est créée en utilisant le chemin d'accès complet et le nom du fichier de configuration du serveur HTTP, où / est remplacé par . .

Par exemple, voici des noms de fichier possibles : Linux AIX

```
khu.usr.local.apache24.conf.httpd.conf
```

Windows

```
khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf
```

Le fichier de configuration du collecteur de données de l'agent HTTP Server contient les éléments suivants :

- Détails sur le chemin d'accès du fichier httpd.conf utilisé par HTTP Server. Par exemple, KhuShmemPath "/IBM/HTTPServer/conf/httpd.conf".
- Emplacement de la bibliothèque à charger
- Droits d'accès associés à la mémoire partagée

Fichier de configuration du serveur HTTP

Chaque serveur HTTP possède un fichier de configuration qui se nomme *rép_install_serveur_http*/conf/httpd.conf par défaut, où *rép_install_serveur_http* désigne le répertoire d'installation du serveur HTTP. Dans certains environnements, ce nom de fichier peut être personnalisé. Vérifiez le nom de fichier exact auprès de l'administrateur du serveur HTTP.

Pourquoi et quand exécuter cette tâche

Activez la collecte de données sur l'agent HTTP Server dans les cas suivants :

- Après avoir installé l'agent HTTP Server
- Après avoir effectué une mise à niveau vers la version 1.0.0.4 de l'agent HTTP Server, le nouvel alias bascule les noeuds existants de l'agent HTTP Server hors ligne dans la console Cloud APM.

- Après avoir effectué une mise à niveau de la version 1.0.0.4, les noeuds existants de l'agent HTTP Server peuvent basculer hors ligne dans la console Cloud APM. Cette situation peut se produire si vous disposez de plusieurs instances du serveur HTTP portant des noms de fichier de configuration d'agent similaires, par exemple `httpd` et `httpd01`.

Important : Pour résoudre ce problème, vous devez ajouter la nouvelle instance du serveur HTTP dans la console Cloud APM une fois cette tâche terminée.

Procédure

1. Pour activer la collecte de données, vous devez référencer le fichier de configuration du collecteur de données dans le fichier de configuration du serveur HTTP en utilisant l'instruction `Include`. Ajoutez l'instruction suivante à la fin du fichier de configuration du serveur HTTP :

   ```
   Include "rép_install/tmp/khu/khu.chemin d'accès complet au nom de fichier de configuration du serveur HTTP.conf"
   ```

   Par exemple,

   Linux AIX Si IBM HTTP Server est installé dans le répertoire `/opt/IBM/HTTPServer` et que le fichier de configuration du collecteur de données se trouve dans le répertoire suivant :

   ```
   /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
   ```

   Ajoutez l'instruction suivante au fichier de configuration du serveur HTTP `/opt/IBM/HTTPServer/conf/httpd.conf` :

   ```
   Include "/opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf"
   ```

   Windows Si un serveur IBM HTTP est installé dans le répertoire `C:\ProgramFiles\IBM\HTTPServer` et que le fichier de configuration du collecteur de données se trouve dans le répertoire

   ```
   C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf,
   ```

   ajoutez l'instruction suivante dans le fichier de configuration du serveur HTTP `C:\Program Files\IBM\HTTPServer\conf\httpd.conf` :

   ```
   Include "C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf"
   ```

2. Accédez au répertoire suivant :

   ```
   répertoire_installation_serveur_HTTP/bin
   ```

3. Redémarrez le serveur HTTP. Par exemple :

   Linux AIX

   ```
   ./apachectl -k stop
   ./apachectl -k start
   ```

   Windows

   ```
   httpd.exe -k stop
   httpd.exe -k start
   ```

Résultats

Vous avez correctement configuré l'agent.

Que faire ensuite

Vous pouvez à présent vérifier que les données de l'agent HTTP Server s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Remarque : Si le trafic est inexistant sur le serveur HTTP, aucune donnée ne s'affichera dans la console Cloud APM.

module IBM HTTP Server Response Time

Lorsque vous installez l'agent Response Time Monitoring pour qu'il fonctionne avec le module IBM HTTP Server Response Time, il surveille les demandes HTTP et HTTPS sur tous les ports.

module IBM HTTP Server Response Time
Le module IBM HTTP Server Response Time fait partie de l'agent HTTP Server. Si l'agent HTTP Server est installé et configuré avant ou en même temps que l'agent Response Time Monitoring sur le serveur Apache HTTP Server ou sur le serveur IBM HTTP Server sous AIX, Linux ou Windows, le module IBM HTTP Server Response Time est automatiquement activé. Pour une description de la fonctionnalité du module IBM HTTP Server Response Time, voir «Configuration du module IBM HTTP Server Response Time», à la page 647.

Fichier de configuration du collecteur de données
Après avoir installé l'agent HTTP Server, ce dernier découvre le serveur HTTP et génère un fichier de configuration du collecteur de données dans le répertoire *rép_install*/tmp/khu, où *rép_install* est le répertoire d'installation de l'agent HTTP Server.

Pour le serveur Apache HTTP Server, le fichier de configuration du collecteur de données est : khu.usr.local.apache24.conf.httpd.conf
Pour le serveur IBM HTTP Server, le fichier de configuration du collecteur de données est : khu.opt.IBM.HTTPServer.conf.httpd.conf

Plug-ins
L'agent HTTP Server est composé de deux plug-ins :

1. khu_module - correspond au agent HTTP Server. Ce plug-in est responsable de tous les tableaux de bord associés à l'agent HTTP Server. Pour plus d'informations, voir agent HTTP Server Reference.
2. wrt_module - correspond au module IBM HTTP Server Response Time

Ces deux plug-ins sont indiqués dans le fichier de configuration de collecteur de données comme suit :

```
LoadModule khu_module
LoadModule wrt_module
```

Activer la collecte de données
Pour activer la collecte de données, vous devez référencer le fichier de configuration du collecteur de données dans le fichier de configuration du serveur HTTP en utilisant l'instruction Include. Ajoutez l'instruction suivante à la fin du fichier de configuration du serveur HTTP :

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 319.

Une fois la collecte de données activée, le tableau de bord de l'utilisateur final est rempli.

Exemples de code pour l'agent HTTP Server

Deux fichiers font partie de la configuration de l'agent HTTP Server. Il s'agit du fichier de configuration du collecteur de données de l'agent HTTP Server et du fichier de configuration du serveur HTTP. Un exemple de fichier de mappage de l'alias d'instance est également fourni pour vous aider à comprendre le fonctionnement d'un alias.

Exemples de fichier du collecteur de données de l'agent HTTP Server

Pour IBM HTTP Server version 8 et ultérieure, 64 bits, le fichier de configuration du collecteur de données de l'agent HTTP Server contient les informations suivantes :

```
#
#Paramètres du module Agent de surveillance pour HTTP Server.
#
```

```
LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_64.so"

<IfModule mod_khu.c>
   KhuShmemPerm 660
   KhuShmemPath "/opt/IBM/IHS/conf/httpd.conf"
   KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22_64.so
WrtOriginID HU:tivvm09_httpd:HUS
```

Pour IBM HTTP Server version 7, 32 bits, le fichier de configuration contient les informations suivantes :

```
#
#Paramètres du module Agent de surveillance pour HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_32.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/opt/IBM/HTTPServer/conf/httpd.conf"
 KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22.so
WrtOriginID HU:linux_httpd:HUS
```

Pour Apache version 2.4, 64 bits, le fichier de configuration de l'agent HTTP Server contient les informations suivantes :

```
#
#Paramètres du module Agent de surveillance pour HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache24dc_64.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/usr/local/apache24/conf/httpd.conf"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  Require all granted
```

```
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap24_64.so
WrtOriginID HU:linux-tzsi_httpd:HUS
```

Exemple de fichier de mappage de l'alias d'instance

```
# Agent de surveillance pour HTTP Server instance alias mapping
# INSTANCE: auto discovered by agent. Please do NOT modify.
# ALIAS: alias name for the instance. The name will be displayed in APM UI dashboard. It must be unique
# among all instances and it must be less than 10 characters and consist of only alphanumeric characters.
#
INSTANCE.1=/usr/local/apache24/conf/httpd.conf
ALIAS.1=httpd

INSTANCE.1=/usr/local/apache24/conf/admin.conf
ALIAS.1=admin
```

Configuration de la surveillance d'IBM Integration Bus

L'agent IBM Integration Bus est un agent multi-instance. Vous devez créer une première instance d'agent et la démarrer manuellement.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 45.

Tableau 45. Versions d'agent

Version d'agent	Documentation
7.3.0.5, 7.3.0.7, 7.3.0.8	Cloud APM 8.1.4
7.3.0.2	IBM Performance Management 8.1.3
7.3.0.1	IBM Performance Management 8.1.2
7.3.0	IBM Performance Management 8.1.1

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent IBM Integration Bus. Pour les toutes dernières informations sur la configuration système requise, voir le rapport détaillé sur la configuration système requise pour l'agent IBM Integration Bus.

Pourquoi et quand exécuter cette tâche

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'agent IBM Integration Bus. Effectuez les étapes nécessaires en fonction de vos besoins.

Procédure

1. Assurez-vous que l'ID utilisateur qui sera utilisé pour démarrer et arrêter l'agent IBM Integration Bus appartient aux groupes d'utilisateurs **mqm** et **mqbrkrs**.
2. Windows Si IBM MQ (WebSphere MQ) est installé sur le système Windows, ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) à la variable d'environnement **PATH**. L'agent IBM Integration Bus pourra ainsi charger les bibliothèques IBM MQ (WebSphere MQ) requises pour démarrer.
   a. Ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) au début de la variable d'environnement **PATH**.

      Par exemple, si le chemin d'installation d'IBM MQ (WebSphere MQ) est `C:\IBM\WMQ75`, ajoutez `C:\IBM\WMQ75\bin` au début de la variable d'environnement **PATH** de votre système Windows.
   b. Redémarrez le système Windows pour que les modifications soient prises en compte.

3. Configurez l'agent IBM Integration Bus en spécifiant les paramètres de configuration suivants. Vous pouvez également spécifier des paramètres de configuration facultatifs pour l'agent. Pour plus d'informations, voir «Configuration de l'agent IBM Integration Bus».
   - ID de l'agent
   - Répertoire d'installation des noeuds d'intégration (courtiers) à surveiller
   - Chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ)
4. Configurez IBM Integration Bus pour activer les données que vous voulez surveiller. Voir «Configuration d'IBM Integration Bus pour l'activation des données», à la page 328.
5. Si vous avez activé la collecte de données d'image instantanée pour votre noeud d'intégration (courtier), configurez l'agent IBM Integration Bus de sorte à ne pas stocker les données d'image instantanée. Pour plus d'informations, voir «Désactivation de la collecte de données d'image instantanée pour l'agent», à la page 332.
6. Facultatif : Pour configurer l'agent IBM Integration Bus afin d'activer le suivi des transactions, utilisez la page Configuration d'agent. Pour plus d'informations, voir «Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 333.
7. Facultatif : Si vous n'avez plus besoin de la fonction de suivi des transactions ou si vous souhaitez désinstaller l'agent IBM Integration Bus, désactivez le suivi des transactions pour IBM Integration Bus et supprimez l'exit utilisateur fourni par l'agent. Pour plus d'informations, voir «Désactivation du suivi des transactions», à la page 331 et «Suppression de l'exit utilisateur KQIUserExit», à la page 334.

Configuration de l'agent IBM Integration Bus

Vous devez attribuer un nom d'instance à l'agent IBM Integration Bus et configurer l'agent pour qu'il puisse commencer à surveiller votre environnement IBM Integration Bus.

Avant de commencer

- Vérifiez que l'ID utilisateur utilisé pour démarrer et arrêter l'agent fait partie des groupes d'utilisateurs **mqm** et **mqbrkrs**.
- Windows Si IBM MQ (WebSphere MQ) est installé sur le système Windows, ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) à la variable d'environnement **PATH**. L'agent IBM Integration Bus pourra ainsi charger les bibliothèques IBM MQ (WebSphere MQ) requises pour démarrer.
  1. Ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) au début de la variable d'environnement **PATH**.

     Par exemple, si le chemin d'installation d'IBM MQ (WebSphere MQ) est `C:\IBM\WMQ75`, ajoutez `C:\IBM\WMQ75\bin` au début de la variable d'environnement **PATH** de votre système Windows.
  2. Redémarrez le système Windows pour que les modifications soient prises en compte.
- Vous devrez peut-être fournir les informations suivantes en fonction de votre environnement au cours de la configuration d'agent. Si vous n'avez aucune idée de la valeur de configuration à spécifier, renseignez-vous auprès de l'administrateur d'IBM MQ (WebSphere MQ) et d'IBM Integration Bus.
  - Si IBM MQ (WebSphere MQ) est installé sur le même système que l'agent IBM Integration Bus, vous devez fournir le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ).
  - S'il est prévu de configurer l'agent IBM Integration Bus pour surveiller les noeuds d'intégration d'IBM Integration Bus V10, vous devez fournir le répertoire d'installation d'IBM Integration Bus V10.
  - Pour que l'agent IBM Integration Bus ne surveille que certains noeuds d'intégration (courtiers) plutôt que tous les noeuds sur le même système, vous devez fournir le nom et le chemin d'installation de chaque noeud d'intégration (courtier).

Pourquoi et quand exécuter cette tâche

L'agent IBM Integration Bus est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement.

Vous pouvez choisir de configurer l'agent avec ou sans interactions sur les systèmes UNIX or Linux. Sur les systèmes Windows, vous pouvez configurer l'agent sans interactions uniquement.

- Pour configurer l'agent avec interaction, exécutez le script de configuration et répondez aux invites. Voir «Configuration interactive».
- Pour configurer l'agent sans interaction, éditez le fichier de réponses silencieux, puis exécutez le script de configuration. Voir «Configuration en mode silencieux», à la page 326.

Important : Si vous avez également installé ITCAM Agent for WebSphere Message Broker, fourni en tant que produit ITCAM for Applications, sur le même système que l'agent IBM Integration Bus, fourni dans Cloud APM, ne les utilisez pas pour surveiller le même noeud d'intégration (courtier) sur le système.

Configuration interactive

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Exécutez la commande suivante :

   ```
   rép_install/bin/iib-agent.sh config nom_instance
   ```

   où *nom_instance* est le nom que vous souhaitez attribuer à l'instance d'agent.
2. Une fois que vous avez confirmé que vous souhaitez configurer l'agent IBM Integration Bus, spécifiez des valeurs de configuration pour les paramètres généraux de l'agent.
   a. Lorsque le système vous invite à indiquer le paramètre **Agent Id**, spécifiez une chaîne alphanumérique unique comportant au maximum 8 caractères.

      Le nom de système géré comprend l'ID agent que vous spécifiez, par exemple, *nom_courtier_surveillé*:*ID_agent*:KQIB, où *nom_courtier_surveillé* est le nom du noeud d'intégration (courtier) surveillé.
   b. Lorsque le système vous invite à indiquer le paramètre **IIB version 10 Install Directory**, si vous souhaitez surveiller les noeuds d'intégration d'IBM Integration Bus V10, spécifiez le répertoire d'installation d'IBM Integration Bus V10. Par exemple, /opt/ibm/mqsi/iib-10.0.0.6. Si vous ne souhaitez pas surveiller IBM Integration Bus V10, appuyez sur Entrée pour accepter la valeur par défaut.

      A faire : Vous ne pouvez spécifier qu'un seul répertoire d'installation pour le paramètre **IIB version 10 Install Directory**. Si vous avez installé IBM Integration Bus V10 dans des répertoires différents et que vous souhaitez surveiller toutes ses instances, créez des instances d'agent multiple et spécifiez un répertoire d'installation d'IBM Integration Bus V10 pour chaque instance d'agent.
3. Facultatif : Utilisez la section **Monitored Broker Settings** pour préciser si cet agent doit surveiller uniquement certains noeuds d'intégration (courtiers).

   Par défaut, tous les noeuds d'intégration (courtiers) exécutés sur le même système hôte que l'agent IBM Integration Bus sont surveillés, comme le détermine la fonction d'auto-reconnaissance. Si vous souhaitez que l'agent surveille certains noeuds d'intégration (courtiers), spécifiez le nom du noeud d'intégration (courtier) que vous souhaitez surveiller et définissez le paramètre **Collect Node Data** sur No (valeur par défaut) dans la section **Monitored Broker Settings**. Il peut y avoir plusieurs sections **Monitored Broker Settings**. Chaque section contrôle les paramètres de surveillance d'un noeud d'intégration (courtier).

   Conseil : Vous pouvez spécifier plusieurs sections **Monitored Broker Settings**. Lorsque vous éditez la section **Monitored Broker Settings**, les options suivantes sont disponibles :

   - Add : créez une section **Monitored Broker Settings** pour configurer un autre noeud d'intégration (courtier).
   - Edit : modifiez les paramètres de la section **Monitored Broker Settings** en cours.
   - Del : supprimez la section **Monitored Broker Settings** en cours.
   - Next : passez à la section **Monitored Broker Settings** suivante.

- Exit : quittez la configuration **Monitored Broker Settings**.

4. Si vous confirmez qu'IBM MQ (WebSphere MQ) est installé sur le même système, vous êtes invité à spécifier le paramètre **WebSphere MQ 64-bit library path**. Appuyez sur Entrée pour accepter la valeur par défaut, qui est le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) automatiquement découvert par l'agent. Si aucune valeur par défaut n'est affichée, vous devez fournir le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour passer à l'étape suivante. Par exemple, `/opt/mqm8/lib64`.

   A faire : Si vos noeuds d'intégration (courtiers) utilisent différentes versions des gestionnaires de files d'attente, indiquez la dernière version du chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour ce paramètre.

5. Une fois la configuration terminée, entrez la commande suivante pour démarrer l'agent :

   rép_install`/bin/iib-agent.sh start`
   nom_instance

Configuration en mode silencieux

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

1. Ouvrez le fichier de réponses silencieux de l'agent ci-après dans un éditeur de texte.

   - Linux AIX *rép_install*`/samples/iib_silent_config.txt`
   - Windows *rép_install*`\tmaitm6_x64\samples\qi_silent_config.txt`

   où *rép_install* correspond au répertoire d'installation de l'agent IBM Integration Bus. Le répertoire d'installation par défaut est le suivant :

   - Linux AIX `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM`

2. Pour le paramètre **agentId**, spécifiez une chaîne alphanumérique unique comportant au maximum 8 caractères qui servira d'identificateur court à l'agent.

   Le nom de système géré comprend l'ID agent que vous spécifiez, par exemple, *nom_courtier_surveillé*`:`*ID_agent*`:KQIB`, où *nom_courtier_surveillé* est le nom du noeud d'intégration (courtier) surveillé.

3. Pour surveiller les noeuds d'intégration (courtiers) d'IBM Integration Bus V10, indiquez le répertoire d'installation d'IBM Integration Bus V10 dans le paramètre **defaultWMBInstallDirectory**. Par exemple, `C:\Program Files\IBM\IIB\10.0.0.6\` pour un système Windows ou `/opt/ibm/mqsi/iib-10.0.0.6` pour un système Linux.

   Si vous ne souhaitez pas surveiller IBM Integration Bus V10, ce paramètre n'est pas obligatoire car l'agent IBM Integration Bus peut découvrir automatiquement les noeuds d'intégration (courtiers) des versions précédentes.

   A faire : Vous ne pouvez spécifier qu'un seul répertoire d'installation pour le paramètre **defaultWMBInstallDirectory**. Si vous avez installé IBM Integration Bus V10 dans des répertoires différents et que vous souhaitez surveiller toutes ses instances, créez des instances d'agent multiple et spécifiez un répertoire d'installation d'IBM Integration Bus V10 pour chaque instance d'agent.

4. Facultatif : Précisez si cet agent doit surveiller uniquement certains noeuds d'intégration (courtiers).

   Par défaut, tous les noeuds d'intégration (courtiers) exécutés sur le même système hôte que l'agent IBM Integration Bus sont surveillés, comme le détermine la fonction d'auto-reconnaissance. Pour surveiller des noeuds d'intégration (courtiers) spécifiques, définissez les paramètres **collectNodeData** et **WMBInstallDirectory** pour chaque noeud d'intégration (courtier) que vous voulez surveiller.

collectNodeData

Indique si les données de définition de noeud sont collectées pour le noeud d'intégration (courtier) surveillé. La syntaxe est `collectNodeData.`*`nom_courtier`*`=NO|YES`, où *nom_courtier* est le nom du noeud d'intégration (courtier).

La valeur par défaut est NO. Il est recommandé d'utiliser la valeur par défaut car les données de définition de noeud ne sont pas prises en charge dans la console Cloud APM.

WMBInstallDirectory

Répertoire d'installation du noeud d'intégration (courtier) à surveiller. La syntaxe est `WMBInstallDirectory.`*`nom_courtier=rép_install_courtier`*, où *rép_install_courtier* est le répertoire d'installation du noeud d'intégration (courtier) à surveiller.

A faire : Pour un noeud d'intégration version 10, le paramètre **WMBInstallDirectory** peut remplacer le paramètre **defaultWMBInstallDirectory** que vous avez défini à l'étape précédente.

Par exemple, pour ne surveiller que deux noeuds d'intégration (courtiers) nommés BK1 et BK2, définissez les paramètres comme suit :

```
collectNodeData.BK1=NO
collectNodeData.BK2=NO
WMBInstallDirectory.BK1=rép_install_BK1
WMBInstallDirectory.BK2=rép_install_BK2
```

5. Pour surveiller les courtiers qui sont antérieurs à la version 10 d'IBM Integration Bus, spécifiez le chemin de la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour le paramètre **WMQLIBPATH**. Par exemple, `C:\Program Files\IBM\WebSphere MQ\bin64` pour un système Windows ou `/opt/mqm8/lib64` pour un système Linux.

   A faire : Si vos noeuds d'intégration (courtiers) utilisent différentes versions des gestionnaires de files d'attente, indiquez la dernière version du chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour ce paramètre.
6. Sauvegardez et fermez le fichier de réponses silencieux de l'agent, puis entrez la commande suivante :
   - Linux AIX *`rép_install`*`/bin/iib-agent.sh config `*`nom_instance chemin_vers_fichier_réponses`*
   - Windows *`rép_install`*`\BIN\iib-agent.bat config "`*`nom_instance chemin_vers_fichier_réponses`*`"`

   où *nom_instance* est le nom de l'instance que vous configurez et *chemin_ fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

   Remarque : Sur les systèmes Windows, n'insérez pas de guillemets ("") qui entourent le chemin d'accès du fichier de réponses silencieux, car cela entraînerait une erreur de configuration.
7. Une fois la configuration terminée, entrez la commande suivante pour démarrer l'agent :
   - Linux AIX

     `rép_install``/bin/iib-agent.sh start `*`nom_instance`*
   - Windows

     `rép_install``\bin\iib-agent.bat start `*`nom_instance`*

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'agent IBM Integration Bus au Tableau de bord d'Application Performance. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

A faire : Chaque fois que vous mettez à jour ou migrez un noeud d'intégration (courtier) surveillé, vous devez redémarrer l'agent IBM Integration Bus après la mise à niveau ou la migration du noeud d'intégration (courtier).

Que faire ensuite

L'étape suivante consiste à configurer IBM Integration Bus pour l'activation des données. Les données suivantes sont disponibles dans le Tableau de bord d'Application Performance uniquement après les avoir activées dans IBM Integration Bus :

- Comptabilité des archives et statistiques
- Statistiques de ressource de la machine virtuelle Java
- Suivi des transactions

Pour plus d'informations, voir «Configuration d'IBM Integration Bus pour l'activation des données».

Configuration d'IBM Integration Bus pour l'activation des données

Pour que certaines données soient disponibles dans la console Cloud APM, vous devez configurer IBM Integration Bus de telle sorte à activer la collecte de données requise.

Avant de commencer

Assurez-vous que l'agent IBM Integration Bus est configuré.

A faire : L'activation du suivi des transactions vous demande de redémarrer le noeud d'intégration (courtier).

Pourquoi et quand exécuter cette tâche

Les statistiques d'archivage et de ressource peuvent être surveillées par l'agent IBM Integration Bus uniquement après avoir activé la collecte de données pour le noeud d'intégration (courtier). De même, si vous souhaitez visualiser le suivi des transactions dans les tableaux de bord de topologie et du middleware, vous devez activer le suivi des transactions au sein du noeud d'intégration (courtier) avant d'activer le suivi des transactions pour l'agent IBM Integration Bus.

Déterminez le type de données que vous voulez surveiller avec l'agent IBM Integration Bus et procédez comme suit en fonction de vos besoins.

Procédure

- Pour activer la collecte des statistiques d'archivage pour le noeud d'intégration (courtier), voir «Activation de la collecte des données statistiques et de comptabilité des archives», à la page 329.
- Pour activer la collecte des statistiques de ressource pour un noeud d'intégration (courtier), voir «Activation des statistiques de ressource de la machine virtuelle Java», à la page 330.
- Pour activer le suivi des transactions pour les flux de messages au sein d'un noeud d'intégration (courtier), voir «Activation du suivi de transaction», à la page 331.
- Si vous ne souhaitez plus de données de suivi des transactions, n'oubliez pas de désactiver le suivi des transactions pour le noeud d'intégration (courtier) sur lequel il a été activé. Voir «Désactivation du suivi des transactions», à la page 331.

Activation de la collecte des données statistiques et de comptabilité des archives

Pourquoi et quand exécuter cette tâche

Pour activer la collecte des statistiques et des données de comptabilité des archives pour les flux de messages qui appartiennent au noeud de courtier d'intégration (courtier), exécutez la commande **mqsichangeflowstats** à partir du répertoire `bin` dans le répertoire d'installation du noeud d'intégration (courtier).

A faire : Emettez la commande **mqsichangeflowstats** au noeud d'intégration (courtier) en fonction de vos besoins en matière de données de surveillance. Il est recommandé d'activer seulement les statistiques nécessaires, car des flux de messages importants génèrent beaucoup de données et de traitement. Pour des informations détaillées sur la commande **mqsichangeflowstats**, reportez-vous à la documentation d'IBM Integration Bus.

Important : IBM Cloud Application Performance Management ne prend pas en charge les données statistiques et de comptabilité des instantanés en raison de la quantité de données et de traitement requise pour l'intervalle de prise d'instantané de 20 secondes défini. Les données d'archive fournissent les mêmes attributs exacts que les données d'instantané et sont plus appropriées pour la surveillance normale de la production fournie par IBM Cloud Application Performance Management. Si vous avez activé la collecte de données d'image instantanée pour le noeud d'intégration (courtier), n'oubliez pas de configurer l'agent IBM Integration Bus de telle sorte à ne pas stocker les données d'image instantanée. Pour plus d'informations, voir «Désactivation de la collecte de données d'image instantanée pour l'agent», à la page 332.

Procédure

- Pour obtenir la plupart des données des flux de messages, exécutez la commande suivante. Cette commande est recommandée car elle n'active pas les statistiques de terminal les plus détaillées, qui fournissent le nombre d'appels par terminal et par noeud. Le niveau de terminal utilise un grand volume de stockage.

  ```
  mqsichangeflowstats nom_courtier -a -g -j -c active -t none -n basic -o xml
  ```

- Pour obtenir toutes les données prises en charge par l'agent IBM Integration Bus, émettez la commande suivante :

  ```
  mqsichangeflowstats nom_courtier -a -g -j -c active -t none -n advanced -o xml
  ```

- Pour réduire la quantité de données mais malgré tout surveiller raisonnablement tous les flux de messages sans d'autres détails, émettez la commande suivante :

  ```
  mqsichangeflowstats nom_courtier -a -g -j -c active -t none -n none -o xml
  ```

- Si vous disposez d'un grand nombre de flux de messages mais voulez réduire la quantité de données, vous pouvez spécifier les flux de messages à surveiller en remplaçant l'option `-g` ou `-j` dans les commandes susmentionnées.
  - Pour spécifier un serveur d'intégration particulier (groupe d'exécution) pour l'activation, remplacez l'option `-g` par `-e` *nom_serveur_intégration*.
  - Pour identifier un flux de messages particulier pour l'activation, remplacez l'option `-j` par `-f` *nom_flux_message*.
  - Si vous avez regroupé vos flux de messages dans des applications, pour spécifier une application particulière pour l'activation, ajoutez l'option `-k` *nom_application* à l'option `-j`.
- L'agent IBM Integration Bus collecte les données statistiques et de comptabilité des archives toutes les 5 minutes. Pour définir l'intervalle auquel le noeud d'intégration (courtier) génère les données statistiques et de comptabilité des archives sur la même valeur, émettez la commande suivante en ayant arrêté le noeud d'intégration (courtier), puis redémarrez le noeud d'intégration (courtier) :

  ```
  mqsichangebroker nom_courtier -v 5
  ```

Résultats

Une fois l'agent IBM Integration Bus configuré et démarré, les données statistiques et de comptabilité des flux de messages s'affichent dans les widgets de groupe suivants :

- Tableau de bord des flux de messages
  - Validations et annulations
  - UC en microsecondes
  - Temps écoulé en microsecondes
  - Débit d'octets d'entrée
  - Débit de messages d'entrée
  - Taille du message d'entrée
  - Temps d'attente UC des messages d'entrée en microsecondes
  - Temps d'attente écoulé des messages d'entrée en microsecondes
  - Erreurs de flux de messages
  - Statistiques sur le noeud de traitement des messages
- Tableau de bord du noeud de traitement
  - UC en microsecondes
  - Temps écoulé en microsecondes
  - Appels
  - Statut du noeud de traitement
  - Statistiques du terminal

Activation des statistiques de ressource de la machine virtuelle Java

Pourquoi et quand exécuter cette tâche

Pour activer les statistiques de ressource de la machine virtuelle Java pour les serveurs d'intégration qui appartiennent au noeud de courtier d'intégration (courtier), exécutez la commande **mqsichangeresourcestats** à partir du répertoire `bin` dans le répertoire d'installation du noeud d'intégration (courtier).

A faire : Les statistiques de ressource de la machine virtuelle Java sont considérées comme facultatives car seuls quelques attributs des données sont affichés par rapport au coût élevé de l'agent qui traite ces données toutes les 20 secondes. Demandez-vous si vous avez vraiment besoin des données statistiques de ressource JVM.

Procédure

- Pour activer les statistiques relatives à tous les serveurs d'intégration dans le noeud d'intégration (courtier), émettez la commande suivante :

  ```
  mqsichangeresourcestats nom_courtier -c active
  ```

- Pour activer les statistiques relatives à un serveur d'intégration donné dans le noeud d'intégration (courtier), émettez la commande suivante :

  ```
  mqsichangeresourcestats nom_courtier -e nom_serveur_intégration -c active
  ```

Résultats

Les données statistiques de ressource JVM sont affichées dans les widgets de groupe suivants :

- Comptage de récupération de place
- Durée de récupération de place
- Mémoire non dynamique de la machine JVM
- Mémoire dynamique de la machine JVM

Activation du suivi de transaction

Avant de commencer

1. Assurez-vous que l'agent IBM Integration Bus est installé. Un exit utilisateur, nommé `KQIUserExit`, est fourni pour activer le suivi des transactions sur IBM Integration Bus.
2. Assurez-vous que l'utilisateur qui démarre le noeud d'intégration (courtier) dispose des droits d'accès au répertoire du module KQI User Exit. En d'autres termes, veillez à ajouter l'ID utilisateur utilisé pour démarrer le noeud d'intégration (courtier) au groupe sous lequel vous avez installé l'agent IBM Integration Bus.

Pourquoi et quand exécuter cette tâche

Vous devez déployer l'exit utilisateur `KQIUserExit` sur le noeud d'intégration (courtier). Sinon, aucune donnée n'est mise à disposition dans les tableaux de bord de middleware et de topologie, même après avoir activé le suivi des transactions sur l'agent IBM Integration Bus.

Conseil : Les noeuds IBM Integration Bus suivants sont inclus dans les tableaux de bord de topologie et du middleware par l'exit utilisateur `KQIUserExit` en tant que services non instrumentés :

- Noeuds de calcul et de base de données où une source de données ODBC est spécifiée
- Noeuds TCP/IP
- Noeuds de fichiers pour serveurs FTP ou FTPS distants
- Noeuds MQ, sauf s'ils sont déjà instrumentés

Procédure

Pour activer le suivi des transactions pour IBM Integration Bus, procédez comme suit :

1. Linux AIX Fermez tous les interpréteurs de commandes de courtier qui ont chargé l'environnement MQSI.
2. Ouvrez la console de commande IBM Integration Bus en utilisant l'une des méthodes suivantes. Si plusieurs versions des noeuds d'intégration (courtiers) sont installées sur votre système, assurez-vous de démarrer la console de commande pour la version appropriée.
   - Windows Cliquez sur **Démarrer** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX A partir du répertoire `bin` du répertoire d'installation du noeud d'intégration (courtier), émettez la commande **mqsiprofile**.
3. Arrêtez le noeud d'intégration (courtier) que vous voulez configurer à l'aide de la commande **mqsistop**.
4. Activez le suivi des transactions pour le flux de messages dans le noeud d'intégration (courtier) en ajoutant l'exit utilisateur KQIUserExit à l'aide de la commande **mqsichangebroker**.
   - Pour activer le suivi des transactions pour tous les flux de messages au sein du noeud d'intégration (courtier), exécutez la commande suivante :

     ```
     mqsichangebroker nom_courtier -e "KQIUserExit"
     ```
   - Pour activer le suivi des transactions pour un flux de messages spécifique au sein du noeud d'intégration (courtier), exécutez la commande suivante :

     ```
     mqsichangeflowuserexits nom_courtier -e nom_groupe_exécution -f nom_flux_messages -a "KQIUserExit"
     ```
5. Redémarrez le noeud d'intégration (courtier) à l'aide de la commande **mqsistart**.

Désactivation du suivi des transactions

Procédure

Pour désactiver le suivi des transactions pour IBM Integration Bus, procédez comme suit :

1. Ouvrez la console de commande IBM Integration Bus en utilisant l'une des méthodes suivantes. Si plusieurs versions des noeuds d'intégration (courtiers) sont installées sur votre système, assurez-vous de démarrer la console de commande pour la version appropriée.
   - Windows Cliquez sur **Démarrer** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX A partir du répertoire `bin` du répertoire d'installation du noeud d'intégration (courtier), émettez la commande **mqsiprofile**.
2. Désactivez le suivi des transactions pour le flux de messages dans un noeud d'intégration (courtier) en utilisant l'une des méthodes suivantes :
   - Pour désactiver le suivi des transactions pour un flux de messages spécifique, utilisez la commande **mqsichangeflowuserexits** :

     ```
     mqsichangeflowuserexits nom_courtier -e nom_groupe_exécution -f nom_flux_messages -a ""
     ```
   - Pour désactiver le suivi des transactions pour tous les flux de messages au sein du noeud d'intégration (courtier), commencez par arrêter le noeud d'intégration (courtier) à l'aide de la commande **mqsistop**, puis émettez la commande **mqsichangebroker** :

     ```
     mqsichangebroker nom_courtier -e ""
     ```

Que faire ensuite

- Pour le suivi des transactions, après avoir activé le suivi des transactions pour IBM Integration Bus, vous devez également activer le suivi des transactions pour l'agent. Pour plus d'informations, voir «Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 333.
- Si vous avez activé la collecte de données d'image instantanée pour votre noeud d'intégration (courtier), configurez l'agent IBM Integration Bus de sorte à ne pas stocker les données d'image instantanée. Cloud APM ne prend pas en charge la comptabilité des instantanés et les données statistiques en raison de la quantité de données et de traitement requise pour l'intervalle de prise d'instantané de 20 secondes défini. Pour plus d'informations, voir «Désactivation de la collecte de données d'image instantanée pour l'agent».

Désactivation de la collecte de données d'image instantanée pour l'agent

Cloud APM ne prend pas en charge la comptabilité des instantanés et les données statistiques en raison de la quantité de données et de traitement requise pour l'intervalle de prise d'instantané de 20 secondes défini. Si vous avez activé la collecte de données d'image instantanée pour le courtier, n'oubliez pas de configurer l'agent IBM Integration Bus pour ne pas stocker les données d'image instantanée.

Procédure

1. Ouvrez le fichier de configuration d'agent dans un éditeur de texte. Le fichier de configuration d'agent se trouve dans l'un des répertoires suivants en fonction du système d'exploitation utilisé :
   - Linux AIX *rép_install*/config/*<nom_hôte>*_qi_*<nom_instance>*.cfg
   - Windows *rép_install*\TMAITM6_x64*<nom_hôte>*_qi_*<nom_instance>*.cfg

   où *rép_install* est le répertoire d'installation d'agent, *nom_hôte* est le nom d'hôte du système d'exploitation et *nom_instance* est le nom d'instance d'agent.
2. Editez le fichier en ajoutant le paramètre suivant dans la section KqiAgent :

   ```
   defaultRetainRecentSnapshotSamples=0
   ```

   Exemple :

   ```
   INSTANCE=inst1 [
   SECTION=KqiAgent [ { agentId=inst1 } { instName=inst1 } {defaultRetainRecentSnapshotSamples=0}]
   SECTION=MonitorBroker:BRK1 [ { collectNodeData=NO } ]
   SECTION=MonitorBroker:BRK2 [ { collectNodeData=NO } ]
   ]
   ```
3. Sauvegardez et fermez le fichier.

4. Redémarrez l'agent IBM Integration Bus pour que les modifications soient prises en compte.

Configuration du suivi des transactions pour l'agent IBM Integration Bus

Les données de suivi des transactions pour IBM Integration Bus peuvent être affichées dans les tableaux de bord de topologie et du middleware une fois la collecte de données activée sur la page Configuration d'agent pour l'agent IBM Integration Bus.

Avant de commencer

- Assurez-vous que le suivi des transactions est activé pour IBM Integration Bus avec l'exit utilisateur fourni par l'agent `KQIUserExit`. Si ce n'est pas fait, suivez les instructions de la rubrique «Activation du suivi de transaction», à la page 331.
- Assurez-vous que l'agent IBM Integration Bus est correctement configuré. Si ce n'est pas fait, suivez les instructions de la rubrique «Configuration de l'agent IBM Integration Bus», à la page 324.

Procédure

Pour configurer le suivi des transactions pour l'agent IBM Integration Bus, procédez comme suit :

1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
2. Cliquez sur l'onglet **IBM Integration Bus**.
3. Cochez les cases des instances d'agent et effectuez l'une des actions suivantes de la liste **Actions** :
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut de la colonne **Transaction Tracking** est mis à jour sur Enabled.
   - Pour désactiver les données de suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut de la colonne **Transaction Tracking** est mis à jour sur Disabled.

Résultats

Vous avez configuré le suivi des transactions pour les instances d'agent sélectionnées. Les données de suivi des transactions peuvent être affichées dans les tableaux de bord de topologie et de middleware une fois que vous avez activé la collecte de données. Pour plus d'informations, voir «Ajout d'applications middleware au Tableau de bord d'Application Performance», à la page 107.

Spécification d'un nom de système géré unique pour agent IBM Integration Bus

Le nom d'instance agent IBM Integration Bus affiché sur la console Cloud APM est également connu comme le nom de système géré. Vous pouvez utiliser le paramètre de configuration d'agent pour indiquer un nom de système géré unique pour chaque instance d'agent.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent IBM Integration Bus est démarré, il enregistre le nom de système géré au format suivant : *nom_courtier_surveillé*:*ID_agent*:KQIB pour chaque instance d'agent, où *nom_courtier_surveillé* est le nom du courtier surveillé et *ID_agent* est l'ID agent défini par le paramètre de configuration d'agent. La longueur maximale du nom de système géré est de 32 caractères. Si la longueur du nom de système géré dépasse ce nombre, le nom est alors tronqué.

Un nom de système géré unique peut être nécessaire dans les cas suivants :

- Plusieurs agents IBM Integration Bus sont en cours d'exécution sur le même système.
- Plusieurs courtiers surveillés du même nom sont en cours d'exécution sur des systèmes différents.

Pour indiquer un ID agent de manière à obtenir un nom de système géré unique, utilisez l'option **ID agent** pendant la configuration interactive ou utilisez le paramètre **agentId** dans le fichier de réponses silencieux.

A faire : Si vous n'avez jamais configuré l'agent IBM Integration Bus suite à l'installation, procédez comme indiqué dans la section «Configuration de l'agent IBM Integration Bus», à la page 324.

Procédure

- Pour utiliser l'option **ID agent** pendant la configuration interactive, procédez comme suit :
  1. Exécutez la commande suivante :

     rép_install/bin/iib-agent.sh config *nom_instance*

     où *nom_instance* est le nom de l'instance d'agent pour laquelle vous souhaitez indiquer un ID agent.
  2. Suivez les options pour configurer l'instance d'agent. Si, pour une option, aucune modification n'est nécessaire, utilisez la valeur par défaut.
  3. Lorsque l'option `ID agent` apparaît, indiquez le qualificateur intermédiaire du nom de système géré. Le format valide est une chaîne alphanumérique comportant au maximum 8 caractères.
- Pour utiliser le paramètre **agentId** dans le fichier de réponses silencieux, procédez comme suit :
  1. Ouvrez le fichier de réponses silencieux de l'agent ci-après dans un éditeur de texte.
     - Linux AIX *rép_install*/samples/iib_silent_config.txt
     - Windows *rép_install*\tmaitm6_x64\samples\qi_silent_config.txt
  2. Indiquez un ID agent pour le paramètre **agentId**. Le format valide est une chaîne alphanumérique comportant au maximum 8 caractères.
  3. Sauvegardez et fermez le fichier de réponses silencieux, puis exécutez la commande suivante à partir de la ligne de commande :
     - Linux AIX *rép_install*/bin/iib-agent.sh config *nom_instance* *chemin_vers_fichier_réponses*
     - Windows *rép_install*\BIN\iib-agent.bat config "*nom_instance* *chemin_vers_fichier_réponses*"

     où *nom_instance* est le nom de l'instance que vous configurez et *chemin_ fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

     Remarque : Sur les systèmes Windows, n'insérez pas de guillemets ("") qui entourent le chemin d'accès du fichier de réponses silencieux, car cela entraînerait une erreur de configuration.
  4. Une fois la configuration terminée, entrez la commande suivante pour démarrer l'agent :
     - Linux AIX

       rép_install/bin/iib-agent.sh start *nom_instance*
     - Windows

       rép_install\bin\iib-agent.bat start *nom_instance*

Que faire ensuite

Connectez vous à console Cloud APM. Si l'instance d'agent portant l'ancien nom de système géré apparaît toujours comme déconnectée, éditez votre application pour la supprimer, puis ajoutez la nouvelle instance d'agent portant l'ID agent attribué.

Suppression de l'exit utilisateur KQIUserExit

Avant de désinstaller l'agent IBM Integration Bus, vous devez commencer par supprimer l'exit utilisateur `KQIUserExit`.

Procédure

Pour supprimer l'exit utilisateur `KQIUserExit` que vous avez déployé sur IBM Integration Bus pour le suivi des transactions, procédez comme suit :

1. Accédez au répertoire `bin` de l'agent IBM Integration Bus.
   - Windows *rép_install_agent*`\arch\qi\bin`
   - Linux AIX *rép_install_agent*`/arch/qi/bin`

   Où :
   - *rép_install_agent* est le répertoire d'installation de l'agent. La valeur par défaut est `C:\IBM\APM` sur les systèmes Windows et `/opt/ibm/apm/agent` sur les systèmes Linux et AIX.
   - *arch* est le code d'architecture de la plateforme. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install_agent*`/archdsc.tbl`.
2. Exécutez le script **`configDC`** pour supprimer la bibliothèque d'exits utilisateur de manière interactive :
   - Windows
     `configDC.bat –disable` *rép_install_iib*
   - Linux AIX
     `./configDC.sh –disable` *rép_install_iib*

   où *rép_install_iib* est le répertoire d'installation d'IBM Integration Bus.

Exemple

L'exemple suivant supprime l'exit utilisateur fourni par l'agent pour les courtiers version 9.0 installés sur un système AIX :

```
cd /opt/IBM/ITM/aix513/qi/bin
./configDC.sh –disable /opt/IBM/mqsi/9.0
```

Configuration de la surveillance d'IBM MQ Appliances

L'Agent MQ Appliance est un agent multi-instance. Après l'installation, vous devez le configurer en créant une instance d'agent pour pouvoir l'utiliser pour la surveillance.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, voir tableau 46.

Tableau 46. Versions d'agent

Version d'agent	Documentation
3.0.0.5	Cloud APM 8.1.4

Procédure

- Sur les systèmes Linux et UNIX, vous pouvez configurer l'agent avec le script de configuration qui génère des invites pour les réponses ou le fichier de réponses silencieux.
  - «Configuration de l'agent en répondant à des invites», à la page 336
  - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 336
- Sur les systèmes Windows, vous pouvez configurer l'agent uniquement avec le fichier de réponses silencieux.
  - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 336

Que faire ensuite

Dans la console Cloud APM, accédez au tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Configuration de l'agent en répondant à des invites

Vous devez attribuer un nom d'instance à Agent MQ Appliance et configurer l'agent pour qu'il puisse commencer à surveiller IBM MQ Appliances.

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Exécutez la commande suivante :

   rép_install`/bin/mq_appliance-agent.sh config` *nom_instance*

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Exemple :

   `/opt/ibm/apm/agent/bin/mq_appliance-agent.sh config AQM904`
2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent MQ Appliance», à la page 337.
3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install`/bin/mq_appliance-agent.sh start` *nom_instance*

   Exemple :

   `/opt/ibm/apm/agent/bin/mq_appliance-agent.sh start AQM904`

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent MQ Appliance au tableau de bord des performances des applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

1. Ouvrez le fichier `mq_appliance_silent_config.txt` dans l'un des répertoires suivants dans un éditeur de texte.
   - Linux AIX *rép_install*`/samples/mq_appliance_silent_config.txt`
   - Windows *rép_install*`\samples\mq_appliance_silent_config.txt`

   où *rép_install* correspond au répertoire d'installation de l'agent. Par exemple, `/opt/ibm/apm/agent`.
2. Dans le fichier `mq_appliance_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent MQ Appliance».
3. Enregistrez et fermez le fichier `mq_appliance_silent_config.txt` et exécutez la commande suivante :
   - Linux AIX

     rép_install`/bin/mq_appliance-agent.sh config` *nom_instance chemin_accès_au_fichier_silencieux*
   - Windows

     rép_install`\bin\mq_appliance-agent.bat config` *nom_instance chemin_accès_au_fichier_silencieux*

   où :
   - *nom_instance* correspond au nom à attribuer à l'instance d'agent. Par exemple, `AQM904`.
   - *chemin_accès_au_fichier_silencieux* correspond au chemin d'accès au fichier `mq_appliance_silent_config.txt`. Par exemple, `/opt/ibm/apm/agent/samples/mq_appliance_silent_config.txt`.
4. Une fois la configuration terminée, exécutez la commande suivante pour démarrer l'agent :
   - Linux AIX

     rép_install`/bin/mq_appliance-agent.sh start` *nom_instance*
   - Windows

     rép_install`\bin\mq_appliance-agent.bat start` *nom_instance*

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent MQ Appliance au tableau de bord des performances des applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

Paramètres de configuration de l'Agent MQ Appliance

Les paramètres de configuration de l'Agent MQ Appliance sont affichés dans des tableaux qui les regroupent par sections.

- tableau 47, à la page 338 : Propriétés pour la réception d'événements SNMP et le décodage des événements V3.
- tableau 48, à la page 338 : Propriétés pour les paramètres Java.
- tableau 49, à la page 339 : Propriétés pour le serveur proxy utilisé par les fournisseurs HTTP.
- tableau 50, à la page 339 : Propriétés pour le serveur HTTP.
- tableau 51, à la page 339 : Propriétés pour la connexion au dispositif MQ.

Tableau 47. Paramètres de configuration d'événement SNMP

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Numéro de port	Numéro de port utilisé pour écouter les événements SNMP. La valeur par défaut est 162.	KQZ_SNMPEVENT_PORT
Niveau de sécurité	Niveau de sécurité utilisé pour la connexion à l'événement SNMP. Il peut correspondre à l'une des valeurs suivantes : • 1=noAuthNoPriv • 2=authNoPriv • 3=authPriv La valeur par défaut est 2.	KQZ_SNMPEVENT_ SECURITY_LEVEL
Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion à l'agent SNMP. La valeur par défaut est snmpuser.	KQZ_SNMPEVENT _USER_NAME
Protocole d'autorisation	Protocole d'autorisation utilisé pour la connexion à l'agent SNMP. Il peut correspondre à l'une des valeurs suivantes : • 1=MD5 • 2=SHA La valeur par défaut est 2.	KQZ_SNMPEVENT_AUTH _PROTOCOL
Mot de passe d'autorisation	Phrase passe d'autorisation utilisée pour la connexion à l'agent SNMP.	KQZ_SNMPEVENT_AUTH _PASSWORD
Mot de passe de confidentialité	Phrase passe de confidentialité utilisée pour la connexion à l'agent SNMP.	KQZ_SNMPEVENT_PRIV _PASSWORD
Fichier de configuration des alertes	Emplacement du fichier de configuration des alertes.	KQZ_SNMPEVENT_ TRAPCNFG_FILE

Tableau 48. Paramètres de configuration Java

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Niveau de trace Java	Niveau de trace utilisé par les fournisseurs Java. Il peut correspondre à l'une des valeurs suivantes : • 1=Arrêt • 2=Erreur • 3=Warning • 4=Information • 5=Débogage minimum • 6=Débogage moyen • 7=Débogage maximum • 8=All La valeur par défaut est 2.	JAVA_TRACE _LEVEL

Tableau 49. Paramètres de configuration du serveur proxy

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Nom d'hôte du proxy	Nom d'hôte du serveur proxy.	KQZ_HTTP _PROXY_HOSTNAME
Port du proxy	Numéro de port du serveur proxy. La valeur par défaut est `80`.	KQZ_HTTP_PROXY_PORT
Nom de l'utilisateur du proxy	Nom d'utilisateur du serveur proxy.	KQZ_HTTP _PROXY_USER
Mot de passe du proxy	Mot de passe du serveur proxy.	KQZ_HTTP _PROXY_PASSWORD

Tableau 50. Paramètres de configuration du serveur HTTP

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Nom d'utilisateur HTTP	Nom d'utilisateur pour l'accès à l'interface MQ Appliance REST Management.	KQZ_HTTP _USER
Mot de passe HTTP	Mot de passe pour l'accès à l'interface MQ Appliance REST Management.	KQZ_HTTP _PASSWORD
Validation des certificats activée	Indique si la validation de certificat est activée. Il peut correspondre à l'une des valeurs suivantes : • 1=true • 2=false La valeur par défaut est `2`.	KQZ_HTTP_CERTIFICATE _VALIDATION

Tableau 51. Paramètres de configuration de la connexion au dispositif MQ

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Hôte ou adresse IP du dispositif	Nom d'hôte ou adresse IP du dispositif MQ. La valeur par défaut est `https://hostnameoripaddress): https://9.123.123.123`	KMK_APPLIANCE _HOST_OR _IP_ADDRESS.arm1
Numéro de port du dispositif	Numéro de port pour la connexion HTTPS au dispositif MQ. La valeur par défaut est `5554`.	KMK_APPLIANCE _PORT_NUMBER.arm1
Nom de l'utilisateur du dispositif	Nom d'utilisateur utilisé pour la connexion au dispositif MQ.	KMK_APPLIANCE _USER_NAME.arm1
Mot de passe de l'utilisateur du dispositif	Mot de passe de l'utilisateur du dispositif MQ.	KMK_APPLIANCE _USER_PASSWORD.arm1
Identification de l'hôte de l'agent	Nom d'hôte du système où Agent MQ Appliance est exécuté. La valeur par défaut est `9.123.123.111`.	KMK_APM_ AGENT_IDENTIFICATION .arm1
Validation des certificats activée	Indique si la validation de certificat est activée pour la connexion HTTP. • 1=true • 2=false La valeur par défaut est `2`.	KMK_CERTIFICATE _VALIDATION_ ENABLED.arm1

Configuration de la surveillance d'InfoSphere DataStage

Vous devez configurer l'Agent DataStage pour la collecte des données de surveillance de la santé et des performances des ressources du serveur DataStage.

Avant de commencer

Pour connaître les prérequis matériels et logiciels, voir Software Product Compatibility Reports for DataStage agent.

Pourquoi et quand exécuter cette tâche

L'Agent DataStage est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**. La fenêtre Monitoring Agent for DataStage s'ouvre.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre Monitoring Agent for DataStage, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 342.
5. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

Que faire ensuite

Définissez la valeur de la première collecte pour visualiser les données comprises dans cet intervalle de temps en secondes au démarrage de l'agent. Effectuez les opérations suivantes :

1. Ouvrez le fichier suivant dans un éditeur :

   rép_install\TMAITM6_x64\KDTENV_*nom_instance*
2. Editez **KDT_FIRST_COLLECTION_INTERVAL**=*intervalle_temps_en_secondes*, où *intervalle_temps_en_secondes* correspond aux données de toutes les exécutions de travaux précédentes dans l'historique à extraire dans le délai spécifié en secondes jusqu'à ce que l'agent démarre. Pour contrôler le volume de données initial, l'utilisateur peut spécifier le paramètre **KDT_FIRST_COLLECTION_INTERVAL** en secondes pour la première collecte. L'agent collecte des données pour les exécutions de travaux qui sont terminées dans la durée spécifiée au cours de l'intervalle de temps spécifié jusqu'à ce que l'agent démarre. Toutes les collectes de données d'agent suivantes pour les exécutions de travaux extraient uniquement les exécutions de travaux récemment ajoutées qui se produisent depuis la dernière collecte.

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur les systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance : `./datastage-agent.sh config nom_instance`
3. Lorsque la ligne de commande affiche le message suivant, tapez 1 et entrez :

   ```
   Edit 'Monitoring Agent for DataStage' setting? [1=Yes, 2=No]
   ```
4. A l'invite, indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 342.
5. Exécutez la commande suivante pour démarrer l'agent :

   ```
   ./datastage-agent.sh start nom_instance
   ```

Que faire ensuite

Définissez la valeur de la première collecte pour visualiser les données comprises dans cet intervalle de temps en secondes au démarrage de l'agent. Effectuez les opérations suivantes :

1. Ouvrez le fichier suivant dans un éditeur :

   rép_install`/config/.dt.environment`
2. Editez **KDT_FIRST_COLLECTION_INTERVAL**=*intervalle_temps_en_secondes*, où *intervalle_temps_en_secondes* correspond aux données de toutes les exécutions de travaux précédentes dans l'historique à extraire dans le délai spécifié en secondes jusqu'à ce que l'agent démarre. Pour contrôler le volume de données initial, l'utilisateur peut spécifier le paramètre **KDT_FIRST_COLLECTION_INTERVAL** en secondes pour la première collecte. L'agent collecte des données pour les exécutions de travaux qui sont terminées au cours de l'intervalle de temps spécifié jusqu'à ce que l'agent démarre. Toutes les collectes de données d'agent suivantes pour les exécutions de travaux extraient uniquement les exécutions de travaux récemment ajoutées qui se produisent depuis la dernière collecte.

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent DataStage sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous

devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de configuration en mode silencieux qui est disponible à l'emplacement suivant et indiquez des valeurs pour tous les paramètres : Windows *rép_install*\samples\datastage_silent_config.txt
   Linux *rép_install*\samples\datastage_silent_config_UNIX.txt
   Windows C:\IBM\APM\samples
   Linux /opt/ibm/apm/agent/samples
   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent».
2. Sur la ligne de commande, modifiez le chemin d'accès sur *rép_install*\bin.
3. Exécutez la commande suivante :
   Windows datastage-agent.bat config *nom_instance rép_install*\samples\datastage_silent_config.txt
   Linux datastage-agent.sh config *nom_instance rép_install*\samples\datastage_silent_config_UNIX.txt
4. Démarrez l'agent.
   Windows Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.
   Linux Exécutez la commande suivante : ./datastage-agent.sh start *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent DataStage, vous pouvez modifier les paramètres de configuration du niveau service, du référentiel de métadonnées ainsi que les paramètres de configuration avancés.

Paramètres de configuration du niveau service

Il s'agit des paramètres de configuration requis pour que l'agent se connecte au niveau service.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du niveau service de l'Agent DataStage.

Tableau 52. Noms et descriptions des paramètres de configuration du niveau service

Nom du paramètre	Description	Zone obligatoire
Nom d'hôte	Nom d'hôte de l'ordinateur sur lequel le niveau service est installé. Si l'ordinateur fait partie d'un domaine, indiquez le nom de domaine complet. La valeur par défaut est localhost.	Oui
Port HTTPS	Port HTTPS de l'interface REST de l'ordinateur sur lequel le niveau service est installé. La valeur par défaut est 9443.	Oui
Nom d'utilisateur WAS	Nom d'utilisateur utilisé pour la connexion à WebSphere Application Server. La valeur par défaut est wasadmin.	Oui

Tableau 52. Noms et descriptions des paramètres de configuration du niveau service (suite)

Nom du paramètre	Description	Zone obligatoire
Mot de passe WAS	Mot de passe utilisé pour la connexion à WebSphere Application Server.	Oui
Confirm WAS Password	Mot de passe indiqué dans la zone **WAS Password**.	Oui

Paramètres de configuration du référentiel de métadonnées

Il s'agit des paramètres de configuration requis pour que l'agent se connecte au référentiel de métadonnées.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du référentiel de métadonnées de l'Agent DataStage.

Tableau 53. Noms et descriptions des paramètres de configuration du référentiel de métadonnées

Nom du paramètre	Description	Zone obligatoire
Type de base de données	Type de la base de données du référentiel de métadonnées. La valeur par défaut pour Db2 est 1.	Oui
Nom d'hôte	Nom d'hôte de l'ordinateur sur lequel le référentiel de métadonnées est installé. Si l'ordinateur fait partie d'un domaine, indiquez le nom de domaine complet. La valeur par défaut est localhost.	Oui
Port de la base de données	Port de la base de données du référentiel de métadonnées utilisé pour la connexion JDBC. La valeur par défaut est 50000.	Oui
Nom d'utilisateur de la base de données	Nom d'utilisateur utilisé pour la connexion à la base de données d'opérations. La valeur par défaut est dsodb.	Oui
Mot de passe de la base de données	Mot de passe utilisé pour la connexion à la base de données d'opérations.	Oui
Confirm Database Password	Mot de passe indiqué dans la zone **Database Password**.	Oui
Chemin de pilote JDBC	Chemin d'accès au pilote JDBC, incluant le fichier jar. Par exemple, /home/jars/db.jar sur le système Linux.	Oui

Paramètres de configuration avancés

Tableau 54. Noms et descriptions des paramètres de configuration avancés

Nom du paramètre	Description	Zone obligatoire
Niveau de trace Java	Niveaux de trace utilisés par les fournisseurs personnalisés Java. La valeur par défaut est 2.	Oui

Paramètres de configuration client de l'interface de programme d'application Java

Tableau 55. Noms et descriptions des paramètres de configuration client de l'interface de programme d'application Java

Nom du paramètre	Description	Zone obligatoire
Chemin d'accès aux classes pour les fichiers JAR		Non

Configuration d'Internet Service Monitor

L'agent Internet Service Monitoring offre la possibilité de déterminer si un service spécifique fonctionne correctement, d'identifier les domaines problématiques et d'établir un rapport sur la performance des services par rapport aux accords sur les niveaux de service. L'agent Internet Service Monitoring fonctionne en émulant les actions d'un utilisateur réel. Il interroge ou teste régulièrement les services Internet pour vérifier leur statut et leurs performances.

Présentation

Lors de la surveillance des services Internet, vous définissez ce qui doit être surveillé, pour qui et quand. Vous pouvez configurer la surveillance des services Internet par le biais de l'interface utilisateur de configuration d'Internet Service Monitoring.

Les moniteurs de service Internet testent les services Internet spécifiques et réacheminent les résultats des tests à Databridge. Les moniteurs émulent les actions d'un utilisateur réel du service.

Par exemple, le moniteur HTTP tente à intervalles réguliers d'accéder à une page Web en émulant les demandes généralement envoyées par un navigateur Web lorsqu'un utilisateur consulte cette page. Le moniteur enregistre le résultat du test, qui est envoyé à la passerelle de données.

Internet Service Monitoring

Chaque moniteur est conçu pour tester un type de protocole ou service. Par exemple, le moniteur HTTP teste la disponibilité des ressources, telles les pages Web via le protocole HTTP, et le moniteur FTP teste le transfert des fichiers entre les hôtes exécutant le protocole FTP.

Un moniteur peut tester plusieurs instances différentes du même service, comme une série de pages Web prises en charge par une plage d'hôtes.

Surveillance des services Web

Grâce à la gamme de moniteurs d'Internet Service Monitoring, vous pouvez personnaliser le type de surveillance des services Web à appliquer, en allant d'une surveillance basique des services Internet testant la disponibilité d'une page Web jusqu'à la combinaison de séquences de tests.

La surveillance des services Internet utilise une grande quantité d'interrogations simples pour tester la disponibilité des services Web. Par exemple, si vous voulez surveiller la disponibilité générale d'un site Web, vous devez utiliser le moniteur HTTP pour interroger un grand nombre d'URL à intervalles réguliers.

A l'aide d'une combinaison de moniteurs, vous pouvez créer un niveau de surveillance de service approprié à la spécification de vos besoins :

- Moniteurs HTTP et HTTPS

  Surveillent la disponibilité des ressources des protocoles HTTP ou HTTPS en exécutant en grande quantité des tests de base à une seule interrogation.
- Moniteur de transactions (TRANSX)

  Combine des séquences de tests effectués par un groupe de moniteurs, simulant ainsi les actions d'un utilisateur réel. Par exemple, se connecter à un service, accéder à un nombre de pages sur plusieurs sites Web, puis accéder aux services de messagerie électronique.

Configuration d'Internet Service Monitoring par le biais de l'interface utilisateur

Pour surveiller les services Internet, créez des profils utilisateur, des éléments de profil et des plannings de surveillance. Configurez des profils utilisateur, des éléments de profil et des plannings de surveillance à l'aide de l'interface utilisateur d'Internet Service Monitoring.

Pourquoi et quand exécuter cette tâche

Un profil utilisateur est un client, un département ou un groupe de services dont vous surveillez les services Internet ou Web. Pour chaque profil utilisateur, l'utilisateur doit définir un ou plusieurs éléments de profil. Par exemple, un utilisateur peut définir un élément de profil pour surveiller une page Web distribuée via un service HTTP ou pour surveiller la disponibilité d'un service FTP. Les profils utilisateur contiennent généralement plusieurs éléments de profil qui testent chacun l'un des services fournis à cet utilisateur. Chaque profil utilisateur dispose également d'une planification de surveillance associée qui détermine le jour et l'heure auxquels s'exécutent les tests définis dans le profil.

Pour accéder à la fenêtre de configuration de l'agent Internet Service Monitoring par le biais du tableau de bord IBM Application Performance Management, procédez comme suit :

Procédure

1. Dans le tableau de bord Application Performance Management, cliquez sur l'icône  . Cliquez sur **Configuration de l'agent**. La fenêtre Configuration de l'agent s'ouvre.
2. Cliquez sur l'onglet **ISM** pour configurer l'agent Internet Service Monitoring.

   L'interface se compose de deux sous-fenêtres. Utilisez la sous-fenêtre de gauche pour créer, éditer, supprimer, actualiser et planifier des profils utilisateur. Utilisez la sous-fenêtre de droite pour déployer les profils utilisateur sur le système géré sélectionné. La version est la version du système géré. Le nom du profil indique le profil utilisateur déployé sur les systèmes gérés sélectionnés. Pour configurer les profils et les déployer sur les systèmes gérés, procédez comme suit.
3. Pour ajouter un profil, cliquez sur l'icône  . Entrez le **Nom de profil** et la **Description** dans la boîte de dialogue.
4. Cliquez sur **Suivant**.
5. Sélectionnez un moniteur dans la liste déroulante et cliquez sur **Suivant**.
6. Indiquez les valeurs des zones et cliquez sur **Ajouter**. Plusieurs moniteurs peuvent être sélectionnés pour un profil. Pour savoir quels moniteurs sont disponibles, voir «Moniteurs Internet Service Monitoring disponibles», à la page 346.
7. Cliquez sur **Terminé**.
8. Cliquez sur l'icône .
9. Pour déployer le profil créé sur un système géré, cochez la case correspondant à ce profil, qui devra être configuré à partir de la sous-fenêtre de gauche, et sélectionnez le nom d'un système géré dans la sous-fenêtre de droite. Cliquez sur **Déployer** pour déployer le profil sur le système géré que vous avez choisi.

Modification des profils

Tous les profils utilisateur créés sont modifiables.

Pourquoi et quand exécuter cette tâche

Pour modifier les profils, procédez comme suit :

Procédure

1. Sélectionnez le **nom du profil** et cliquez sur  .
2. Sélectionnez un service à modifier et cliquez sur **Suivant**.
3. Modifiez les valeurs pour le service sélectionné.

   Remarque :

- Pour pouvoir modifier la zone du mot de passe, cliquez deux fois sur la zone de texte **nom d'utilisateur**. L'utilisateur peut modifier ou ajouter un nom d'utilisateur et modifier le mot de passe.
- Pour pouvoir modifier la zone **sslkeypassword**, cliquez deux fois sur son texte pour modifier la clé confidentielle.

4. Cliquez sur **Sauvegarder**, puis sur l'icône pour actualiser l'écran.

Programmation d'un profil

Les profils créés peuvent être planifiés en vue de leur déploiement à une date et heure données.

Pourquoi et quand exécuter cette tâche

Pour planifier les profils, procédez comme suit :

Procédure

1. Sélectionnez le **nom du profil**.
2. Cliquez sur le bouton **Planifier**.
3. Planifiez le profil en sélectionnant le jour en face de l'heure. L'utilisateur peut faire glisser la grille pour sélectionner une heure voulue.
4. Cliquez sur **Sauvegarder**.
5. Cliquez sur l'icône pour actualiser l'écran.

Suppression d'un profil

Les profils créés peuvent être supprimés définitivement.

Pourquoi et quand exécuter cette tâche

Pour supprimer le profil, procédez comme suit :

Procédure

1. Sélectionnez le **nom du profil**.
2. Cliquez sur l'icône pour supprimer le profil.

Moniteurs Internet Service Monitoring disponibles

L'ensemble des moniteurs Internet Service Monitoring couvre une large gamme de services Internet.

Le tableau suivant répertorie les moniteurs disponibles avec l'agent Internet Service Monitoring et les types de service surveillés.

Tableau 56. Moniteurs de service Internet disponibles

Nom de contrôleur	Type de service contrôlé
DHCP	Dynamic Host Configuration Protocol. Pour configurer DHCP, voir tableau 61, à la page 357.
DNS	Domain Name Service. Pour configurer DNS, voir tableau 66, à la page 360.
FTP	File Transport Protocol. Pour configurer FTP, voir tableau 71, à la page 363.
HTTP	HyperText Transport Protocol. Pour configurer HTTP, voir tableau 76, à la page 369.
HTTPS	HyperText Transport Protocol (Secure). Pour configurer HTTPS, voir tableau 82, à la page 376.

Tableau 56. Moniteurs de service Internet disponibles (suite)

Nom de contrôleur	Type de service contrôlé
IMAP4	Internet Message Access Protocol. Pour configurer IMAP4, voir tableau 87, à la page 382.
POP3	Post Office Protocol. Pour configurer POP3, voir tableau 92, à la page 386.
ICMP	Internet Control Message Protocol. Pour configurer ICMP, voir tableau 97, à la page 390.
TCPPort	Transmission Control Protocol. Pour configurer TCPPort, voir tableau 102, à la page 395
SMTP	Simple Mail Transport Protocol. Pour configurer SMTP, voir tableau 107, à la page 399.
TRANSX	Transactions. Pour configurer TRANSX, voir tableau 112, à la page 404.

Fichiers

Fichier exécutable

Chaque moniteur de service Internet est constitué d'un fichier exécutable, d'un fichier de propriétés, d'un fichier de règles et d'un fichier journal.

Les fichiers exécutables du moniteur se trouvent dans le répertoire `$ISHOME/platform/arch/bin`. La valeur `arch` est le code d'architecture du système d'exploitation Windows - `win 32`.

Fichier de propriétés

Le fichier des propriétés est un fichier texte qui comporte des paramètres par défaut précédés du symbole dièse.

Pour modifier un paramètre, vous pouvez soit modifier le paramètre par défaut et supprimer le dièse, soit copier et coller la ligne contenant le paramètre au-dessous des paramètres par défaut, puis effectuer la modification et supprimer le symbole dièse. Cela permet de restaurer les valeurs par défaut ultérieurement. Les fichiers de propriétés du moniteur se trouvent dans le répertoire `$ISHOME/etc/props`.

Fichier de règles

Les fichiers de règles sont similaires aux fichiers de règles de sonde IBM Application Performance Management Netcool/OMNIbus. Pour plus d'informations sur leur syntaxe, reportez-vous au document *IBM Application Performance Management Netcool/OMNIbus Probe and Gateway Guide*.

Les fichiers de règles du moniteur se trouvent dans le répertoire `$ISHOME/etc/rules`.

Fichier journal

Les fichiers journaux stockent les messages concernant l'opération du moniteur.

Les fichiers journaux du moniteur se trouvent dans le répertoire `$ISHOME/log`. La propriété `MessageLog` détermine l'emplacement et le nom du fichier journal. La propriété `MessageLevel` sélectionne le niveau d'information écrit sur le fichier journal, par exemple, les messages de débogage détaillés ou les messages d'erreur fatale. La propriété `MaxLogFileSize` détermine la taille du fichier journal avant le report.

Le nom par défaut du fichier journal est `nom.log` où *nom* correspond au nom du moniteur.

Fonctions communes :

Un certain nombre de fonctions sont communes à tous les moniteurs de services Internet. Elles incluent des propriétés, les résultats produits par les moniteurs et les messages d'état.

Cette section décrit les propriétés de tous les moniteurs. Les propriétés de moniteurs spécifiques sont décrites dans la section dédiée au moniteur individuel.

Les paramètres de propriété par défaut sont mis en évidence dans le tableau suivant, le cas échéant.

Tableau 57. Propriétés communes

Nom de la propriété	Paramètre de la propriété	Description
AddRoute	0|1	Crée une route entre l'adresse IP de l'interface réseau utilisée par le moniteur et l'adresse IP de l'hôte surveillé. 0 - désactivé 1 - activé (le moniteur utilise la route spécifiée dans l'élément de profil et non une autre interface réseau). **Remarque :** Cette propriété n'est pas prise en charge sur les plateformes AIX et HP-UX.
BridgeIPAddress	non applicable	Indique l'adresse IP du Databridge. Cette propriété n'est pas configurable ; le Databridge se trouve toujours sur l'hôte local.
BridgePort	entier	Numéro de port utilisé par le Databridge. Définissez cette propriété sur une valeur identique à celle de la propriété SocketPort du Databridge. Valeur par défaut : 9510
BridgeSSLAuthenticatePeer	0|1	Si vous voulez configurer l'authentification SSL entre le moniteur et le pont ou entre le pont et l'agent, définissez BridgeSSLAuthenticatePeer sur 1 et redémarrez le pont. Cette action permet d'authentifier les certificats du serveur. Des certificats sont stockés dans BridgeSSLTrustStore. 0 - désactivé 1 - activé
BridgeSSLCertificateFile	chaîne	Indique le chemin et le nom de fichier du certificat SSL Bridge numérique. Valeur par défaut : $ISHOME/certificates/monitorCert.pem
BridgeSSLCipherSet	chaîne	Définit un ensemble de chiffrements. Si vous modifiez cette valeur, utilisez la syntaxe de chiffrement définie dans la documentation OpenSSL. **Remarque :** Définissez la même valeur sur l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : RC4:3DES:DES:+EXP
BridgeSSLDisableSSLv2	0|1	Détermine quels types de socket sont acceptés. • Si elle est définie sur 0, SSLv2 et SSLv3 sont acceptés. • Si elle est définie sur 1, seuls des sockets SSLv3 sont ouverts. **Restriction :** Définissez la même valeur sur l'agent Internet Service Monitoring, tous les moniteurs et Databridge.

Tableau 57. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`BridgeSSLEncryption`	`0`|`1`	Active le chiffrement SSL Bridge. Définissez cette propriété sur une valeur identique à celle de la propriété Databridge correspondante. `0` - désactivé `1` - activé **Remarque :** Définissez la même valeur pour tous les moniteurs.
`BridgeSSLKeyFile`	chaîne	Chemin et nom du fichier de clé privée SSL Bridge. Valeur par défaut : `$ISHOME/certificates/monitorKey.pem`
`BridgeSSLKeyPassword`	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL Bridge. Valeur par défaut : `tivoli`
`BridgeSSLTruststore`	chaîne	Chemin et nom du fichier de certificat sécurisé pour l'authentification. Nécessaire uniquement lorsque le paramètre `BridgeSSLAuthenticatePeer` est utilisé. Si vous voulez configurer l'authentification SSL entre le moniteur et le pont ou entre le pont et l'agent, définissez `BridgeSSLAuthenticatePeer` sur `1` et redémarrez le pont. Cette action permet d'authentifier les certificats du serveur. Vous pouvez stocker des certificats dans `SSLTrustStoreFile` et `SSLTrustStorePath`. Valeurs par défaut : • `SSLTrustStoreFile`, `$ISHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISHOME/certificates/` Pour ajouter de nouveaux certificats, effectuez l'une des étapes suivantes : • Ajoutez un certificat à la fin de la liste dans le fichier texte `SSLTrustStoreFile`. • Ajoutez un certificat au répertoire `SSLTrustStorePath` et exécutez la commande OpenSSL `c_rehash` *`rép_certificat`* pour hacher les certificats.
`BridgeTimeout`	entier	Délai d'attente, en secondes, par le moniteur d'une réponse du Databridge.
`ConfigFile`	chaîne	Utilisé pour pointer vers un fichier de configuration de surveillance. Valeur par défaut : blanc (chaîne vide).
`ConfigurationCheckInterval`	entier	Intervalle (en secondes) auquel le moniteur recherche des modifications du profil. Valeur par défaut : 1

Tableau 57. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`Datalog`	`0`|`1`	Oblige le moniteur à consigner les données de performance dans un fichier datalog. Les données de performance sont consignées dans :`$ISHOME/datalogs/`*`profil_utilisateur`* `0` - désactivé `1` - activé
`DatalogFormat`	chaîne	Définit le format du fichier datalog. Le paramètre est une liste d'éléments séparés par des espaces, dont les valeurs doivent être stockées dans le fichier datalog. Pour chaque interrogation, le résultat est écrit dans le fichier datalog, l'heure en cours (`$time`) et la durée (`$totalTime`) sont consignées, suivies de tous les éléments définis dans cette propriété.
`DatalogNameFormat`	chaîne	Format du nom de fichier datalog.
`Domain`	chaîne	Indique le nom de domaine de l'hôte exécutant le moniteur. Si cette propriété n'est pas définie, le moniteur tente de déterminer le nom de domaine à l'aide des configurations NIS et DNS.
`DumpProps`	non applicable	Affiche une liste de toutes les propriétés d'un moniteur.
`FullHostInfo`	`0`|`1`	Indique si l'élément `$host` doit être mappé à un élément d'adresse IP `$hostIP` (si `$host` est un nom DNS) ou à un élément de nom DNS (si `$host` est une adresse IP). `0` - désactivé `1` - activé **Remarque :** Non disponible dans le moniteur TRANSX.
`GroupID`	chaîne	ID de groupe sous lequel le moniteur doit être exécuté.
`Aide`	`0`|`1`	Affiche l'aide des options de ligne de commande sans exécuter le moniteur. `0` - désactivé `1` - activé
`IdentifierChecksumFields`	chaîne	Déprécié.
`IgnoreUnmatchedDVC`	`0`|`1`	Si une classification de niveau de service particulière n'obtient pas de correspondance (élément non créé par le moniteur), ignorez cet élément dans le calcul du niveau de service. **Conseil :** Dans les versions précédentes de Internet Service Monitoring, les classifications de niveau de service étaient appelées DVC (Discrete Value Classifications). `0` - désactivé `1` - activé

Tableau 57. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`IpAddress`	chaîne	Indique l'adresse IP de l'interface réseau utilisée par le moniteur pendant les tests. Si cette propriété n'est pas définie, le moniteur tente de déterminer l'adresse IP de la machine hôte à l'aide d'une recherche de nom d'hôte. Cette tentative peut échouer si la machine hôte possède plusieurs interfaces réseau.
`Manager`	chaîne	Indique le nom de l'application de gestion utilisée dans la déduplication de l'événement ObjectServer.
`MaxCCA`	entier	Définit le nombre maximal de connexions simultanées que peut avoir le moniteur à un moment donné. Notez que si vous définissez une valeur trop élevée, vous pouvez gravement affecter les performances du moniteur. Cette propriété n'est pas disponible pour le moniteur ICMP. Valeur par défaut : `10`
`MaxLogFileSize`	entier	Taille maximale (en octets) du fichier journal. Valeur par défaut : `1 048 576`
`MessageLevel`	chaîne	Niveau le plus grave des messages à envoyer au journal des messages. Les valeurs, par ordre croissant de gravité sont : `debug`, `info`, `warn`, `error` et `fatal`. Valeur par défaut : `warn`
`MessageLog`	chaîne	Emplacement du fichier journal. Valeur par défaut : `$ISHOME/log/`*`moniteur`*`.log`
`MinPoll`	entier	Définit l'intervalle d'interrogation minimum autorisé. Si les fichiers de configuration de surveillance ont un intervalle d'interrogation inférieur à la valeur définie, la valeur du fichier de configuration est substituée. Valeur par défaut : `60`
`MsgDailyLog`	entier	Active la génération d'un fichier journal quotidien. Valeur par défaut : `0` - Journal quotidien désactivé
`MsgTimeLog`	chaîne	Indique l'heure (au format 24 heures `HHMM`) après laquelle le moniteur génère un journal quotidien, si MsgDailyLog est activée. Valeur par défaut : `0000` - 12 minuit
`Nom`	chaîne	Nom du moniteur. Définir cette propriété rétablit la valeur par défaut des propriétés `PropsFile`, `RulesFile` et `MessageLog`.

Tableau 57. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`NewProfileCheckMultiple`	entier	Multiple qui indique la fréquence à laquelle le moniteur vérifie les nouveaux fichiers de configuration lorsqu'il vérifie les modifications de profil. Valeur par défaut : `10`
`NoRecover`	entier	Ordonne au moniteur de ne pas récupérer le fichier SAF. Valeur par défaut : `0` - la reprise n'est pas supprimée
`Pause`	entier	Définit l'intervalle (en secondes) auquel un moniteur génère des unités d'exécution. La définition de cette propriété sur des valeurs élevées, 100 ou plus par exemple, force le moniteur à générer des unités d'exécution à une fréquence inférieure. En règle générale, augmenter cette valeur n'est nécessaire que sur des systèmes lents. Cette propriété n'est pas prise en charge pour le moniteur ICMP. Valeur par défaut : `50`
`PreviousFields`	chaîne	Les éléments indiqués par cette propriété (au format "`<element>, <element>, ...`") sont stockés pour un sondage et précédés de la chaîne `previous`.
`Profile`	chaîne	Nom du ou des profils client à utiliser. La chaîne peut être un nom de profil unique, une liste de noms de profils séparés par des espaces ou un astérisque (`*`) qui force le moniteur à utiliser tous les profils disponibles. Valeur par défaut : `*`
`ProfileUpdateTimeout`	entier	Nombre de millisecondes pendant lesquelles un fichier de profil doit rester statique avant de pouvoir être lu par un moniteur, puis mis à jour. La plage autorisée est comprise entre `1-20000` millisecondes. Valeur par défaut : `100`
`PropsFile`	chaîne	Nom du fichier de propriétés. Valeur par défaut : `$ISHOME/etc/props/`*`moniteur`*`.props`
`QFile`	chaîne	Définit le nom du fichier SAF. Valeur par défaut : `$ISHOME/var/`*`moniteur`*`.saf`.
`QSize`	entier	Définit la taille réservée (en octets) du fichier SAF. Valeur par défaut : `10240000`

Tableau 57. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`ID utilisateur`	chaîne	ID utilisateur sous lequel le moniteur doit être exécuté. **Remarque :** N'utilisez pas cette propriété avec le moniteur DHCP.
`Version`	non applicable	Imprime la version du moniteur sans exécuter ce dernier.

Eléments de moniteur communs :

Cette section décrit les éléments générés par tous les moniteurs. Les éléments propres à un moniteur sont décrits dans les sections consacrées à chaque moniteur. Les éléments produits peuvent être affichés dans le tableau de bord de l'agent Internet Service Monitoring.

Si vous utilisez IBM Application Performance Management, les éléments pouvant être affichés dans les espaces de travail en tant qu'attributs sont déterminés par un fichier de mappage généré par l'agent Internet Service Monitoring. Ce fichier de mappage n'est pas configurable.

Le tableau 58 répertorie les éléments générés par tous les moniteurs. Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs d'espace de travail. Les noms des attributs sont affichés entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe pas d'attribut d'espace de travail équivalent. Les attributs placés entre parenthèses mais sans élément indiquent qu'ils sont disponibles uniquement en tant qu'attributs d'espace de travail, il n'existe pas d'élément équivalent.

Tableau 58. Eléments de moniteur communs

Nom de l'élément.	Description de l'élément
`$consecutiveFailures`	Si la valeur `$failureRetests` est différente de zéro et que le test échoue en termes de classification du niveau de service, cet élément est créé à partir de la valeur 1. La valeur augmente jusqu'à ce que le test n'échoue plus, point auquel `$consecutiveFailures` est défini sur `0`, ou jusqu'à l'interrogation suivante. Si, lors de cette interrogation, le niveau de service est atteint ou recommence à augmenter, l'élément n'est plus créé. Si la valeur de cet élément dépasse la valeur de `$failureRetests`, la valeur de `$consecutiveFailures` revient à 1. **Remarque :** Le moniteur TRANSX ne génère pas cet élément.

`$datalogPath*`
 	
`(guid)`
	Chemin du fichier datalog utilisé par le moniteur. L'attribut d'espace de travail utilise les 100 derniers caractères du chemin.

`$description*`
 	
`(Description)`
	Contient la description sous forme de texte fournie dans la zone **Description** de l'élément de profil du moniteur.

`$failureRetestInterval`	Intervalle d'interrogation utilisé lors de la nouvelle tentative de test de l'incident. Ce paramètre est valide uniquement si `$failureRetests` a une valeur supérieure à `0`. Si l'intervalle de nouveau test est supérieur à l'intervalle d'interrogation normal, il redevient égal à ce dernier. **Remarque :** Le moniteur TRANSX ne génère pas cet élément.
`$failureRetests`	Nombre d'incidents de niveau de service à dépasser avant qu'un événement ayant échoué soit enregistré et envoyé à ObjectServer. **Remarque :** Le moniteur TRANSX ne génère pas cet élément.

Tableau 58. Eléments de moniteur communs (suite)

Nom de l'élément.	Description de l'élément
$host* (Host)	Nom de l'hôte ou du serveur. Il est stocké dans le fichier de configuration.
$hostName	Contient le nom d'hôte de l'élément $host (si $host est une adresse IP).
$hostIP	Contient l'adresse IP hôte de $host (si $host est un nom DNS).
$identchecksum* (Identchecksum)	Identificateur de l'élément de profil.
$lastServiceLevel* (LastServiceLevel)	Numéro de niveau de service de l'interrogation précédente. Cette valeur est effacée si le profil change.
$lastServiceLevelCounter	Elément serviceLevelCounter de l'interrogation précédente. Cette valeur est redéfinie si le profil est modifié.
$monitorDNSdomain	Nom de domaine de la machine exécutant le moniteur, tel qu'il est utilisé par le système de noms de domaine.
$monitorHost* (MonitorLocation)	Nom de l'hôte exécutant le moniteur.
$monitorNISdomain	Nom de domaine de l'hôte exécutant le moniteur, tel qu'il est utilisé par NIS (Network Information Service).
$monitorDomain	Remplace les paramètres $monitorDNSdomain et $monitorNISdomain.
$message* (ResultMessage)	chaîne de texte décrivant le résultat de l'interrogation. Par exemple, Echec de la connexion, OK ou Réussite.
(Node)	Nom du système sur lequel Internet Service Monitoring s'exécute. Cet attribut est ajouté par l'agent Internet Service Monitoring.
$pollInterval	Intervalle d'interrogation spécifié dans chaque moniteur.
$resultString* (ResultString)	Chaîne de texte indiquant la classification des niveaux de services appliquée aux résultats de l'interrogation. Par exemple, TotalTime > 20.
$service* (Service)	Nom du service surveillé. Par exemple, FTP ou HTTP.
$serviceLevel* (ServiceLevel)	Numéro du niveau de service de l'interrogation, tel qu'il est défini dans la classification des niveaux de services : 0 - Unknown 1 - Good 2 - Marginal 3 - Failed
$serviceLevelCounter	Nombre de fois que le numéro du niveau de service n'a pas changé.
(ServiceLevelString)	Chaîne associée au niveau de service renvoyé (Unknown, Good, Marginal ou Failed).
$startTimePoll	Heure de début de l'interrogation.
$time	Heure UNIX, en secondes, à laquelle l'interrogation a été effectuée.
$timeStamp* (Timestamp)	Date et heure d'exécution du test. Le format d'horodatage utilise des paramètres locaux.

Tableau 58. Eléments de moniteur communs (suite)

Nom de l'élément.	Description de l'élément
`$transxName`	Nom de la transaction. Il est généré par un moniteur si celui-ci est utilisé dans une transaction.
Détails du profil	

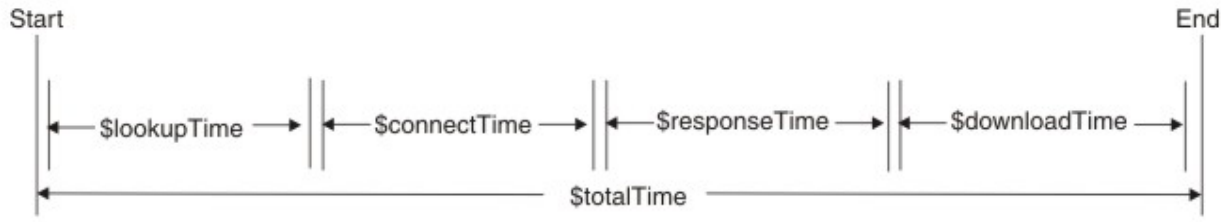
`$profile*`
 	
`(IsmProfile)`
	Nom du profil utilisateur.

Durées - Pour plus d'informations sur la méthode de mesure des durées, voir «Calculs des délais».	
`$timeout`	Délai de réponse du serveur, en secondes. Extrait du fichier de configuration.

`$totalTime*`
 	
`(TotalTime)`
	Durée totale, en secondes, nécessaire à l'exécution d'une opération. Elle inclut toutes les durées de consultation, de connexion et de téléchargement le cas échéant, ainsi que le temps de traitement intermédiaire.

Calculs des délais

Les moniteurs tentent de diviser le délai nécessaire à l'exécution d'une interrogation en différentes étapes temporisées. Par exemple, cela peut inclure le délai nécessaire à l'obtention de l'adresse IP d'un hôte ou le délai nécessaire à l'aboutissement de la connexion à un hôte.



La durée `$totalTime` est toujours légèrement supérieure à la somme des autres durées car elle inclut le temps système utilisé par les activités du moniteur, telles que le traitement des données reçues et l'exécution d'appels système. `$totalTime` est exprimé en secondes.

Messages d'état :

Les moniteurs renvoient les messages d'état générés après chaque test du service. Ils indiquent le résultat des tests.

Les messages proviennent généralement du service surveillé ou de l'environnement réseau extérieur au moniteur. Le tableau 59, à la page 356 décrit les messages d'état communs renvoyés par les moniteurs dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Les messages d'état propres à un moniteur sont décrits dans les sections consacrées à chaque moniteur.

Outre les messages fournis par chaque moniteur, certains moniteurs (le moniteur HTTP, par exemple) signalent les messages du système d'exploitation sous-jacent. Par exemple, si la connexion TCP échoue, Internet Service Monitoring utilise la chaîne définie par le système d'exploitation, telle que **`connection refused`**, **`timeout`**, **`network unreachable`**.

Tableau 59. Messages d'état communs

Message	Description
`OK`	La demande émanant du moniteur a abouti. Les moniteurs peuvent avoir d'autres messages d'état qui indiquent l'aboutissement d'un processus. Reportez-vous à la section *Messages d'état* de chaque moniteur.
`Received response to request not originating from this monitor - ignored`	Le système a reçu une réponse du serveur à un message qui ne provient pas du moniteur désigné.

`Connection failed`
 	
`Connect to server failed`
	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, reportez-vous au fichier journal.

`Connection closed unexpectedly`	La connexion au serveur a été interrompue.
`Connection timed out`	La connexion a abouti mais le serveur a cessé de répondre.
`Connection closed by foreign host`	L'hôte distant a fermé la connexion plus tôt que prévu par le moniteur.
`Timed out waiting to read/write`	Une connexion de données au serveur surveillé a été établie, mais elle a cessé de répondre.
`No Response from server`	Délai d'attente de la demande dépassé.

`Format Error`
 	
`Server Failure`
 	
`No such host or domain`
 	
`Not Implemented`
 	
`Request refused`
 	
`Erreur inconnue`
	Erreur renvoyée par le serveur surveillé.

`Network is down`
 	
`Network is unreachable`
 	
`Network dropped connection on reset`
 	
`Software caused connection abort`
 	
`Connection reset by peer`
 	
`Connection timed out`
 	
`Connection refused`
 	
`Host is down`
 	
`No route to host`
 	
`Remote peer released connection`
	Un incident a été détecté sur le réseau.

Moniteur DHCP :

Le moniteur DHCP vérifie la disponibilité et le temps de réponse des serveurs DHCP.

Vous affectez les classifications de niveau de service selon le temps nécessaire au serveur DHCP pour répondre à une demande du moniteur DHCP à l'aide du temps total, de recherche ou de réponse.

Tableau 60. Fichiers du moniteur DHCP

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_dhcp`
Fichier de propriétés	`$ISMHOME/etc/props/dhcp.props`
Fichier de règles	`$ISMHOME/etc/rules/dhcp.rules`
Fichier journal	`$ISMHOME/log/dhcp.log`

Consignes de configuration du moniteur DHCP

Le moniteur DHCP teste les services DHCP en se comportant comme un client DHCP limité. Il envoie une demande DHCP INFORM au serveur DHCP cible sur le même réseau en utilisant UDP en tant que protocole de transport via une connexion établie et attend un accusé de réception DHCP correspondant du serveur. Le moniteur ne demande pas d'adresse IP et n'affecte pas l'expiration sur des adresses IP existantes.

Remarque : Les serveurs DHCP surveillés doivent prendre en charge les demandes DHCP INFORM et être compatibles RFC2131.

Le moniteur DHCP doit être exécuté en tant que `root` car il est associé à un port inférieur à 1024.

Limitation

Le moniteur DHCP ne peut utiliser aucune interface réseau configurée à l'aide d'un client DHCP. Il doit être configuré pour utiliser une interface réseau dont l'adresse IP n'est pas affectée dynamiquement.

Configuration du test du service de surveillance DHCP

Tableau 61. Configuration du moniteur DHCP

Zone	Description
server	Nom d'hôte du serveur DHCP. Par exemple : dhcp1.mycompany.com
localip	Interface réseau de l'adresse IP utilisée par le moniteur pour effectuer le test. Par exemple : 192.168.n.n
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple : moniteur DHCP
port	Numéro de port du serveur DHCP ; la valeur par défaut est 67.
localport	Numéro de port utilisé par le moniteur pour effectuer le test ; la valeur par défaut est 68.
timeout	Délai d'attente, en secondes, d'une réponse du serveur ; la valeur par défaut est 30.
retries	Nombre de tentatives de connexion au serveur DHCP que le moniteur doit effectuer avant d'arrêter. La valeur par défaut est 0. Exemple : 2.
poll	Délai, en secondes, entre chaque interrogation du serveur utilisant l'élément de profil en cours. La valeur par défaut est 300.
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. La valeur par défaut est 0.
retestinterval	Délai, en secondes, entre chaque nouveau test en cas d'incident. La valeur par défaut est 30.

Outre les résultats de test communs à tous les éléments, le moniteur DHCP génère un ensemble de résultats de test contenant les données propres aux tests de service DHCP.

Tableau 62. Eléments du moniteur DHCP

Elément	Description
`$clientIP*ClientIp`	Adresse IP de l'hôte sur lequel le moniteur s'exécute.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$responseTime*ResponseTime`	Délai entre l'établissement de la connexion et la réception du premier octet de données.
`$retries`	Nombre maximal d'entrées, tel que spécifié pendant la configuration du moniteur.
`$router`	Adresse IP du routeur telle que renvoyée par le serveur DHCP.

Messages d'état

Le moniteur DHCP fournit des messages d'état dans l'attribut `ResultMessage` lorsqu'IBM Application Performance Management est utilisé. Ces messages indiquent le résultat du test.

Tableau 63. Messages d'état du moniteur DHCP

Message	Description
`Received DHCPACK Received DHCPNAK`	Un serveur DHCP a répondu à la demande d'informations DHCP envoyée par le moniteur.
`This monitor requires root privileges to run`	Connectez-vous en tant que superutilisateur.
`Did not receive valid DHCP MESSAGE`	Réponse non reconnue du serveur DHCP.
`Did not receive valid DHCP MESSAGE TYPE`	Réponse non reconnue du serveur DHCP (`DHCPACK` ou `DHCPNAK` était attendue).
`Invalid transaction IDReceived response to request not originating from this monitor - ignored`	Une réponse à un message ne provenant pas de ce moniteur a été reçue d'un serveur DHCP .
`Unexpected op-code returned`	Un message imprévu a été reçu sur ce port.
`Connection failed`	Le nom du serveur spécifié n'est pas valide.
`Failed to send request to DHCP server`	Le système d'exploitation ne peut pas identifier précisément la raison pour laquelle la demande n'a pas pu être transmise au serveur et renvoie donc cette erreur générale indiquant qu'un problème de réseau s'est produit.
`No Response from server`	Le serveur DHCP ne répond pas.

Moniteur DNS :

Le moniteur DNS utilise le service DNS (Domain Name System) pour trouver des informations sur un ou plusieurs hôtes.

Le moniteur DNS utilise soit l'adresse IP de l'hôte pour rechercher le nom de l'hôte, soit le nom de l'hôte pour rechercher l'adresse IP. Le moniteur mesure la performance du service en enregistrant le résultat de la recherche et les temps de réponse. Le moniteur enregistre également des détails sur chaque demande envoyée au serveur.

Tableau 64. Récapitulatif des fichiers du moniteur DNS

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_dns`

Tableau 64. Récapitulatif des fichiers du moniteur DNS (suite)

Fichiers du moniteur	Nom ou emplacement
Fichier de propriétés	`$ISMHOME/etc/props/dns.props`
Fichier de règles	`$ISMHOME/etc/rules/dns.rules`
Fichier journal	`$ISMHOME/log/dns.log`

Consignes de configuration du moniteur DNS

Le moniteur DNS peut être configuré pour rechercher l'adresse IP ou le nom d'hôte de l'hôte cible. En fonction du type de recherche, le moniteur communique avec le serveur DNS différemment.

Recherche d'adresse IP

Lors d'un test de recherche d'adresse IP, un nom d'hôte est attribué au moniteur. Ce nom permet de définir l'emplacement d'une adresse IP.

Le moniteur teste le serveur DNS de la manière suivante :

1. Le moniteur interroge le serveur DNS en utilisant le nom d'hôte complet de HostA (`hosta.dev.net`) pour demander son adresse IP.

   Si le serveur DNS peut définir l'emplacement de l'adresse IP de l'hôte, il est renvoyé au moniteur. Si le serveur DNS ne peut définir l'emplacement de l'adresse IP de l'hôte, il renvoie un message contenant les détails de l'échec de la recherche au moniteur.

   Si la demande arrive à expiration, le moniteur fait de nouvelles tentatives (si de nouvelles tentatives sont configurées). Lorsque toutes les nouvelles tentatives ont été effectuées, le moniteur crée un événement ayant échoué.

   Si le nom d'hôte indiqué dans la configuration est un nom de domaine, tel que `mycompany.com` et non un nom d'hôte qualifié complet, tel que `hostx.mycompany.com`, le moniteur extrait des informations sur l'intégralité du domaine. Ces informations sont stockées dans deux éléments supplémentaires : `$domainNameServer` et `$domainNameAddr`.
2. Si le message renvoyé au moniteur contient un nom canonique, le moniteur en déduit que le nom indiqué dans le fichier de configuration devait être un alias. Le moniteur envoie le nom canonique au serveur DNS afin de demander l'adresse IP de l'hôte.

   Si le serveur DNS définit l'emplacement de l'adresse IP de l'hôte à l'aide de son nom canonique, il est renvoyé au moniteur. Si le serveur DNS ne peut définir l'emplacement de l'adresse IP de l'hôte, il renvoie un message contenant les détails de l'échec de la recherche au moniteur.
3. Si les deux premières tentatives d'interrogation du serveur DNS n'aboutissent pas, le moniteur envoie l'adresse IP du serveur DNS (`192.168.n.n`) au serveur DNS et demande son nom qualifié complet.

   Si le serveur DNS peut définir l'emplacement de son nom d'hôte complet, ce dernier est renvoyé au moniteur. Si le serveur DNS ne peut définir l'emplacement de son nom d'hôte complet, il renvoie un message contenant les détails de l'échec de la recherche. La demande du nom d'hôte qualifié complet du serveur (une demande de recherche DNS inversée), n'est pas prise en charge sur tous les types de serveurs DNS. Si le serveur DNS cible ne prend pas en charge les recherches inversées, vous pouvez empêcher le moniteur DNS d'envoyer cette demande en définissant la propriété `LookupServerName` sur `0`.

Recherche récursive

Les recherches non récursives présentent une vue précise du mode de fonctionnement du serveur DNS alors que les recherches récursives offrent une meilleure indication des performances DNS obtenues par les applications Internet (et donc les utilisateurs). Le moniteur DNS prend en charge les recherches récursives et non récursives.

Les applications Internet font généralement fonctionner les requêtes DNS de cette manière. Par exemple, un navigateur Web spécifie toujours des recherches récursives lorsqu'il tente de résoudre la partie hôte d'une URL.

Si un serveur DNS ne peut pas répondre à une requête parce que sa base de données ne contient pas d'entrée pour l'hôte, il peut périodiquement interroger les serveurs DNS situés plus hauts dans la hiérarchie.

Types de requête DNS

Le moniteur DNS prend en charge plusieurs types de requête DNS. Utilisez le code de requête lors de la spécification du type de requête DNS.

Tableau 65. Types de requête DNS

Code de requête	Type de requête
A	Host Address
NS	Authoritative name server
MD	Mail destination
MF	Mail forwarder
CNAME	Canonical name for an alias
SOA	Start of a zone of authority
MB	Mailbox domain name
MG	Mail group member
MR	Mail rename domain name.
NULL	Null RR
WKS	Well known service description
PTR	Domain name pointer
HINFO	Host information
MINFO	Mailbox or mail list information
MX	Mail exchange
TXT	Text strings
AXFR	Transfer of an entire zone
MAILB	Mailbox-related records
MAILA	Mail agent RR
ANY	All records

Configuration des tests de service du moniteur DNS

Les paramètres de configuration du moniteur DNS permettent de définir les tests de service DNS.

Tableau 66. Tableau 3. Configuration du moniteur DNS

Zone	Description
server	Adresse IP du serveur DNS principal. Par exemple, 192.168.n.n
host	Nom d'hôte de l'hôte cible. Par exemple, www.mycompany.com
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, moniteur DNS.

Tableau 66. Tableau 3. Configuration du moniteur DNS (suite)

Zone	Description
recursivelookups	Active ou désactive les recherches récursives. • `recurse` (utilisez `true` dans ismbatch) • `norecurse` (utilisez `false` dans ismbatch) Valeur par défaut : `recurse`.
port	Port du serveur DNS que le moniteur écoute et dont la valeur par défaut est 53.
localip	Spécifie l'adresse IP de l'interface réseau sur la machine hôte à laquelle le moniteur est associé lorsqu'il effectue le test. Si la propriété `IpAddress` du moniteur est définie, elle remplace la valeur de cette zone.
querytype	Type de requête DNS utilisé dans le test. Pour une liste des types de requête pris en charge, voir tableau 65, à la page 360.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `10`.
retries	Nombre de tentatives du moniteur pour contacter le serveur DNS avant d'abandonner.
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`.
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`.
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`.

Eléments de contrôle

Outre les résultats de test communs à tous les éléments, le moniteur DNS génère un ensemble de résultats de test contenant les données propres aux tests de service DNS.

Tableau 67. Tableau 4. Eléments du moniteur DNS

Elément	Description
`$authoritative`	Cet élément est créé uniquement si les informations récupérées proviennent d'un serveur DNS de référence. S'il ne s'agissait pas d'un serveur DNS de référence, cet élément n'est pas créé.
`$domainEmailAddr`	Adresse de contact du domaine cible.
`$domainNameServer`	Nom du serveur DNS pour le domaine cible.
`$fromAliasTime`	Durée entre l'émission d'une demande de nom conique, reçu depuis une demande précédente, et la réception d'une adresse IP.
`$localIP`	Adresse IP locale que le moniteur doit utiliser. Cet élément peut être vide sur une machine ayant une seule interface.
`$lookup*(HostLookup)`	Nom d'hôte ou adresse IP de l'hôte cible dont le moniteur tente de définir l'emplacement.
`$lookupCName`	Nom d'hôte officiel de l'hôte cible. Cet élément est créé uniquement si le nom d'hôte officiel est différent du nom d'hôte de `$lookupName`.
`$lookupIP*(HostIp)`	Adresse IP de l'hôte cible.
`$lookupName*(Host)`	Nom d'hôte complet de l'hôte cible.
`$mxRecords`	Nombre d'enregistrements MX trouvés.

Tableau 67. Tableau 4. Eléments du moniteur DNS (suite)

Elément	Description
$port	Port sur lequel le service est surveillé.
$queryType	Type de requête DNS utilisée dans le test. Pour une liste des types de requête pris en charge, Voir tableau 65, à la page 360.
$responseTime*(ResponseTime)	Durée entre l'émission par le moniteur d'une demande au serveur DNS et la réception d'une réponse.
$retries	Nombre maximal de nouvelles tentatives, comme indiqué dans l'élément de profil.
$serverIP	Adresse IP du serveur DNS.
$serverName	Nom d'hôte du serveur DNS.
$serverTime	Temps que le serveur passe pour résoudre son propre nom.

Gestion des enregistrements MX

Deux éléments sont créés pour chaque enregistrement MX trouvé par le moniteur DNS : $mxHostn et $mxPreferencen.

$mxHostn stocke le nom d'hôte d'un enregistrement MX. $mxPreferencen contient la préférence de pondération de l'hôte. Le n augmente pour chaque paire d'enregistrement afin de les différencier. Le moniteur stocke le nombre total d'enregistrements MX pour un hôte spécifique dans l'élément $mxRecords. Les paires d'enregistrements sont triées dans l'ordre décroissant des préférences MX.

Message d'état

Le moniteur DNS fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Tableau 68. Tableau 5. Messages d'état du moniteur DNS

Message	Description
Domain information received	Demande de nom de domaine effectuée.
Success	Demande effectuée.
Invalid Response	Réponse non reconnue du serveur DNS.
Connection failed	Le nom du serveur spécifié n'est pas valide.
No Response from server	Délai d'attente de la demande dépassé.
Failed to send DNS request	Un incident a été détecté sur le réseau.
No such domain (no recursion)	Nom de domaine incorrect.

Propriétés

Les propriétés spécifiques au moniteur DNS sont décrites dans le tableau suivant.

Tableau 69. Propriétés du moniteur DNS

Nom de la propriété	Paramètre de la propriété	Description
AcceptCNAME	0|1	Si elle est activée, le moniteur DNS accepte le nom canonique contenu dans la réponse DNS et n'effectue pas d'autres recherches.
DNSQueryType	chaîne	Type de requête DNS utilisée dans les tests. Voir tableau 65, à la page 360 pour une liste des types de requête pris en charge. Valeur par défaut : ANY.

Tableau 69. Propriétés du moniteur DNS (suite)

Nom de la propriété	Paramètre de la propriété	Description
LookupServerName	0|1	Active la recherche DNS inversée sur l'adresse IP du serveur DNS. 0 - désactivé 1 - activé

Moniteur FTP :

Le moniteur FTP teste les services FTP en téléchargeant des fichiers vers ou à partir de serveurs FTP. Il surveille la performance du service en enregistrant le temps de réponse et les taux de transfert des données et surveille l'espace du disque et l'intégrité du fichier.

Tableau 70. Récapitulatif du moniteur FTP

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	nco_m_ftp
Fichier de propriétés	$ISHOME/etc/props/ftp.props
Fichier de règles	$ISHOME/etc/rules/ftp.rules
Fichier journal	$ISHOME/log/ftp.log

Consignes de configuration du moniteur FTP

Le moniteur FTP teste la disponibilité d'un serveur FTP en téléchargeant un fichier sur le serveur à l'aide d'une commande FTP STOR ou en téléchargeant un fichier à partir du serveur à l'aide d'une commande FTP RETR.

Configuration des tests de service du moniteur FTP

Les paramètres de configuration du moniteur FTP sont décrits dans le tableau suivant.

Tableau 71. Configuration du moniteur FTP

Zone	Description
server	Adresse IP du serveur FTP cible ou de la machine à partir de laquelle récupérer des données via FTP. Par exemple : ftp.mycompany.com
localfile	Pour les opérations GET FTP, cette zone spécifie le nom et le chemin vers lequel le fichier est téléchargé. Pour les opérations PUT FTP, cette zone spécifie le nom et le chemin du fichier qui est chargé sur le serveur FTP. La valeur par défaut est FULL PATHNAME. Par exemple : $ISMHOME/etc/ism/downloads/ftp-test.tar.Z
remotefile	Pour les opérations GET FTP, cette zone spécifie le nom et le chemin du fichier téléchargé à partir du serveur. Pour les opérations PUT FTP, cette zone spécifie le nom et le chemin vers lequel le fichier est chargé sur le serveur FTP. La valeur par défaut est FULL PATHNAME. Par exemple : /sales/prodlist.tar.Z
description	Zone de texte dans laquelle placer des informations descriptives sur l'élément.

Tableau 71. Configuration du moniteur FTP (suite)

Zone	Description
port	Port par défaut utilisé par le serveur FTP. Port par défaut : `21`
username	Nom d'utilisateur permettant de se connecter au serveur FTP cible.
password	Mot de passe permettant de se connecter au serveur FTP cible. Ne remplissez pas cette zone si le compte FTP ne requiert pas de mot de passe.
command	Commande FTP pour le moniteur à utiliser : • `GET` ou `RECV` - Téléchargement d'un fichier à partir du serveur FTP cible • `SEND` ou `PUT` - Chargement d'un fichier vers le serveur FTP cible Valeur par défaut : `GET`.
conntype	Spécifie le type de connexion pour le moniteur afin d'établir une connexion au serveur lors de la tentative de transfert du fichier : • `Rapports actifs` • `Passif` Valeur par défaut : `Actif`
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`.
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`.
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`.

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur FTP tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Les expressions régulières effectuent la correspondance de chaînes pour le contenu téléchargé lors des tests de service. Ces expressions peuvent contenir un ou plusieurs opérateurs d'expression réguliers, qui déterminent le contenu à vérifier par l'expression.

Remarque : La syntaxe de l'expression régulière peut être utilisée pour correspondre à des chaînes sur des lignes uniques seulement. Internet Service Monitoring ne peut pas établir de correspondance avec des chaînes qui incluent de nouvelles lignes ou des retours chariot. Utilisez plusieurs expressions régulières pour établir des correspondances avec des chaînes qui s'étendent

sur plusieurs lignes. Vous pouvez également utiliser des règles SLC pour déclencher des alarmes en fonction du résultat de plusieurs expressions régulières.

Tableau 72. Opérateurs génériques

Caractère	Description
.	Correspond à un caractère. Par exemple, l'expression régulière `r.t` correspond aux chaînes `rat`, `rut`, `r t`, mais non à `root`.
$	Correspond à la fin d'une ligne. Par exemple, l'expression régulière `dog$` correspond à la fin de la chaîne `it's a dog` mais non à la chaîne `There are a lot of dogs`.
^	Correspond au début d'une ligne. Par exemple, l'expression régulière `^When in` correspond au début de la chaîne `When in the course of human events` mais non à `What and When in the`.
*	Ne correspond à aucune occurrence ou à plusieurs occurrences du caractère précédant. Par exemple, l'expression régulière `.*` correspond à un nombre indéfini de caractères.
\	Traite le caractère suivant en tant que caractère ordinaire. Par exemple, `\$` correspond au caractère dollar `$` et non à la fin d'une ligne. De même, l'expression `\.` correspond au point et non à un seul caractère.
[]	Correspond à un des caractères compris entre crochets. Par exemple, l'expression régulière `r[aou]t` correspond à `rat`, `rot`, et `rut` mais non à `rit`. Indiquez des plages de caractères en utilisant un tiret. Par exemple, l'expression régulière `[0-9]` correspond à tout chiffre. Vous pouvez également spécifier plusieurs plages. Par exemple, l'expression régulière `[A-Za-z]` correspond à toute lettre en minuscule ou majuscule.
|	Correspond à des phrases contenant une des conditions spécifiées. Par exemple, `him|her` correspond à la ligne `it belongs to him` et à la ligne `it belongs to her`, mais non à la ligne `it belongs to them`.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur FTP génère un ensemble de résultats de test contenant les données propres aux tests de service FTP.

Tableau 73. Eléments du moniteur FTP

Elément	Description
`$bytesPerSec*(BytesPerSec)`	Nombre moyen d'octets transférés par seconde.
`$bytesTransfered*(BytesTransferred)`	Nombre d'octets transférés ou téléchargés.
`$checksum`	Généralement, l'élément Checksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de car les valeurs de total de contrôle sont inconnues au moment de la création de l'élément de profil (le moniteur calcule les valeurs de total de contrôle pendant l'exécution des tests). Les éléments de moniteur $checksum et $previousChecksum sont destinés à l'amélioration des alertes à l'aide du fichier de règles du moniteur.
`$command*(FtpCommand)`	Commande FTP émise par le moniteur.

Tableau 73. Eléments du moniteur FTP (suite)

Elément	Description
`$connectionType*(FtpConnection)`	Type de connexion de données utilisé. Il peut s'agir de `ACTIVE` ou de `PASSIVE`.
`$connectTime*(ConnectTime)`	Temps mis pour se connecter au serveur FTP.
`$downloadTime`	Temps mis pour télécharger le fichier.
`$localFile*(FtpLocalFile)`	Nom de chemin complet du fichier stocké sur l'hôte local. Cet élément est tiré du fichier de configuration.
`$lookupTime*(LookupTime)`	Temps mis pour rechercher l'adresse IP du serveur FTP.
`$previousChecksum`	Généralement, l'élément PreviousChecksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de total de contrôle sont inconnues au moment de la création de l'élément de profil (le moniteur calcule les valeurs de total de contrôle pendant l'exécution des tests). Les éléments de moniteur $previousChecksum et $checksum sont destinés à l'amélioration des alertes à l'aide du fichier de règles du moniteur.
`$regexp`*n*	Expression régulière.
`$regexpMatch`*n*	Contenu de la ligne correspondant à l'expression régulière.
`$regexpStatus`*n*	Etat de la correspondance des expressions régulières : `NONE` - Aucune vérification d'expression régulière n'est configurée `MATCHED` - une correspondance a été trouvée pour l'expression régulière `FAILED` - aucune correspondance n'a été trouvée pour l'expression régulière
`$remoteFile*(FtpRemoteFile)`	Nom de chemin complet du fichier stocké sur l'hôte distant (serveur FTP). Cet élément est tiré du fichier de configuration.
`$responseTime*(ResponseTime)`	Délai entre l'établissement d'une connexion et la réception du premier octet du fichier cible.
`$status`	Code d'état renvoyé par le serveur FTP.
`$transferTime*(TransferTime)`	Définit la valeur sur `$uploadTime` ou `$downloadTime`.
`$uploadTime`	Temps mis pour charger le fichier.
`$username`	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion à l'hôte cible. Cet élément est issu du fichier de configuration si `$message` contient `OK`.

Messages d'état

Le moniteur FTP fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Tableau 74. Messages d'état du moniteur FTP

Message	Description
`OK`	Demande FTP effectuée.
`Unable to open local file for reading/writing`	Voir le fichier journal du moniteur FTP pour plus d'informations.
`Unable to read from/write to local file`	
`Unable to read from data connection`	Une connexion de données au serveur FTP a été établie, mais un incident s'est produit.
`Unable to upload to ftp server`	
`Timed out waiting to read/write`	
`Connection closed by foreign host`	Connexion au serveur FTP rompue.
`Connection closed unexpectedly`	
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur FTP. Voir le fichier journal du moniteur FTP pour plus d'informations.

Moniteur HTTP :

Le moniteur HTTP vérifie la disponibilité et le temps de réponse des serveurs Web.

Il peut surveiller des pages Web individuelles, y compris celles utilisant l'interface CGI, qui nécessite normalement que l'utilisateur entre des données dans des zones. Il peut également surveiller le temps de téléchargement des éléments tels que les images sur une page Web.

Tableau 75. Récapitulatif des fichiers du moniteur HTTP

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_http`
Fichier de propriétés	`$ISHOME/etc/props/http.props`
Fichier de règles	`$ISHOME/etc/rules/http.rules`
Fichier journal	`$ISHOME/log/http.log`

Consignes de configuration du moniteur HTTP

Les moniteurs HTTP et HTTPS vérifient la disponibilité et le temps de réponse des serveurs Web. Utilisez le moniteur HTTP dans les situations suivantes :

- Le site Web cible est statique.

  Pour les sites Web dynamiques, utilisez le moniteur TRANSX.
- Le site Web cible est pris en charge via le protocole HTTP.

  Pour les sites Web qui fournissent du contenu via le protocole HTTPS, sélectionnez le moniteur HTTPS.
- Pour effectuer la surveillance sur plusieurs plateformes.
- La vitesse est un facteur déterminant (le moniteur HTTP offre des performances élevées).

Types de requête HTTP

Le moniteur HTTP émule un navigateur Web qui prend en charge le protocole HTTP/1.0. Pour tester le serveur Web, le moniteur envoie une requête pour une page Web à l'aide des types de requête HTTP suivants :

- `HEAD`

  La commande `HEAD` tente d'accéder à une page Web et de renvoyer l'en-tête HTTP. L'émission de la commande `HEAD` permet de vérifier rapidement qu'une page Web est accessible.
- `GET`

  La commande `GET` tente d'accéder à la page Web et de renvoyer l'ensemble de la page, notamment l'en-tête HTTP. Elle ne tente pas de renvoyer les fichiers associés à cette page, tels que les images.
- `GETALL`

  La commande `GETALL` tente d'accéder à la page Web et renvoie l'ensemble de la page, notamment l'en-tête HTTP, l'arrière-plan, les images, les applets, les cadres, les fichiers CSS et les scripts. Tout comme les commandes `HEAD` et `GET`, cette commande vérifie également qu'une page Web est accessible, mais étant donné que la commande `GETALL` renvoie l'ensemble de la page et tous ses fichiers associés, elle peut donner une indication plus réaliste de la durée nécessaire pour l'accès à la page. Le moniteur utilise également plusieurs unités d'exécution lors d'une commande `GETALL` pour une correspondance plus précise du comportement des navigateurs Web.
- `POST`

La commande POST tente d'accéder à une page Web qui contient un formulaire HTTP et de compléter les zones de ce dernier. Ajoutez le corps de texte de la requête POST dans l'onglet **Corps** de la configuration d'Internet Service Monitoring ou utilisez le groupe @Body de la configuration d'Internet Service Monitoring ou ismbatch. Vous pouvez également utiliser les paramètres FORM. En revanche, vous ne pouvez pas utiliser les paramètres Corps de texte et FORM dans la demande POST.

Utilisation d'un serveur proxy

Vous pouvez tester la disponibilité des pages Web via un serveur proxy. Lorsque vous configurez le moniteur afin qu'il utilise un proxy, il envoie des demandes HTTP via le proxy. Si nécessaire, vous pouvez ignorer le cache de proxy. Vous pouvez configurer les paramètres pour le serveur proxy dans l'onglet **Détails du proxy**. Le moniteur HTTP prend en charge l'accès authentifié aux serveurs proxy. Cette authentification est indépendante de toute authentification requise pour la page Web cible.

Eléments du serveur proxy

Dans les versions antérieures, lorsque vous configuriez un élément de profil de sorte qu'il utilise un serveur proxy, le moniteur HTTP insérait par défaut le nom et le port du serveur proxy dans les éléments $server et $port, au lieu du nom et du port du serveur de destination prévu. Pour conserver la valeur du nom et du port du serveur de destination prévu dans les versions antérieures, définissez la propriété generateProxyTokens sur 1 ou démarrez le moniteur avec le paramètre de ligne de commande -generateproxytokens.

En plus de conserver les valeurs des éléments $server et $port lorsque cette propriété ou ce paramètre de ligne de commande est défini, le moniteur génère les éléments $proxyServer, $proxyPort, $proxyAuthType, $proxyUsername et $proxyCache.

Authentification

Si la page Web que vous souhaitez surveiller ou le serveur proxy que vous souhaitez tester nécessite une authentification, entrez les données d'identification permettant d'accéder à la page dans les zones de paramètre authenticationtype, username et password sur l'onglet Avancé ou Détails du proxy.

Pour désactiver l'authentification, attribuez la valeur NONE à authenticationtype.

Pour sélectionner l'authentification de base, procédez comme suit :

1. Attribuez la valeur BASIC à authenticationtype.
2. Attribuez la valeur username et password aux éléments requis par la page web ou le serveur proxy.

Pour sélectionner NTLM, procédez comme suit :

1. Attribuez la valeur NTLMv1 ou NTLMv2 à authenticationtype.
2. Attribuez la valeur username et password aux éléments requis par la page web ou le serveur proxy.

Remarque :

Le moniteur limite la longueur des requêtes HTTP à 4096 caractères. Si la longueur des données de formulaire supplémentaires est à l'origine d'une longueur de demande qui dépasse cette limite, le moniteur n'inclut pas les données de formulaire supplémentaires dans la demande.

Configuration du test de service du moniteur HTTP

Les paramètres de configuration du moniteur HTTP permettent de définir les tests de service HTTP.

Tableau 76. Configuration du moniteur HTTP

Zone	Description
server	Nom d'hôte du serveur à surveiller. Par exemple, `www.mycompany.com`
page	URL de la page à surveiller. Par exemple, `index.html`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, `surveillance via un serveur proxy`
port	Port du serveur HTTP à utiliser. Valeur par défaut : `80`
localip	Indique l'adresse IP de l'interface réseau utilisée par le moniteur pour le test. Si cette zone est vide, le moniteur utilise l'interface spécifiée par la propriété `IpAddress`.
version	Version de protocole HTTP à utiliser : • `1.0` • `1.1` Valeur par défaut : `1.0`
command	Type de requête HTTP : • `HEAD` • `GET` • `GETALL` • `POST` Valeur par défaut : `GET`
formname	Lorsqu'il est utilisé dans une transaction, le moniteur HTTP recherche dans le formulaire spécifié les valeurs par défaut. Toute valeur trouvée est automatiquement insérée dans l'étape HTTP suivante de la transaction.
authenticationtype	Spécifie le mécanisme d'authentification par stimulation/réponse des utilisateurs réseau : • `NONE` - Aucune authentification • `BASIC` • `NTLMv1` - Authentification par demande/réponse Windows NTLM version 1 • `NTLMv2` - Windows NTLM version 2 Valeur par défaut : `NONE`
username	Nom d'utilisateur (nom de compte) du moniteur à utiliser pour se connecter au serveur.
password	Mot de passe correspondant au nom d'utilisateur du moniteur à utiliser pour la connexion au serveur.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`.
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Tableau 76. Configuration du moniteur HTTP (suite)

Zone	Description
verifycertificate	Désactivé par défaut.
Caractéristiques du proxy	
server	Nom d'hôte du serveur proxy.
port	Port du serveur proxy à utiliser. Valeur par défaut : `8080`
authenticationtype	Type d'authentification pour le serveur proxy. Pour plus d'informations, voir `authenticationtype` ci-dessus. Valeur par défaut : `NONE`
username	Elément utilisé par le moniteur avec le mot de passe pour établir la connexion au serveur proxy.
password	Elément utilisé par le moniteur avec le nom d'utilisateur pour établir la connexion au serveur proxy et dont le libellé est mot de passe.
useproxy	Configure le moniteur pour exécuter la demande en utilisant un serveur proxy. • `proxy` (utilisez `true` dans ismbatch) • `noproxy` (utilisez `false` dans ismbatch) Valeur par défaut : `noproxy`
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • `default` définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • `4Then6` sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • `6Then4` sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • `4Only` sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • `6Only` sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • `6Or4` sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.
nocache	Défini par défaut sur cache.

Expression régulière

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur HTTP tente de faire correspondre le contenu extrait à chaque expression régulière. Si une correspondance à une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service. Pour plus d'informations sur la syntaxe des expressions régulières, voir tableau 72, à la page 365.

Paramètre d'en-tête et de formulaire

Le moniteur HTTP peut envoyer des données supplémentaires dans les zones d'en-tête et dans le corps de message des requêtes HTTP.

Vous pouvez configurer les paramètres de ces données supplémentaires sur l'onglet Paramètres. Les paramètres sont Nom, Valeur et Type, et fonctionnent de la manière suivante :

- Les paires Nom/Valeur de type HEAD spécifient des zones d'en-tête supplémentaires, telles que `User-Agent` et `Referer`, incluses dans toutes les demandes HTTP envoyées par le moniteur. Les zones d'en-tête peuvent être définies pour tout type de méthode HTTP (`GET`, `GETALL`, `HEAD` ou `POST`).

  Pour ITCAM for Transactions version 7.4.0.1 et versions ultérieures, le paramètre HEAD de l'agent utilisateur par défaut `Mozilla/5.0 (ISM-MONITOR)` est ajouté à chaque nouvel élément HTTP ou HTTPS. L'en-tête de l'agent utilisateur par défaut est ajouté de sorte que les moniteurs HTTP et HTTPS puissent être utilisés avec les sites Web pour lesquels le contenu est fonction du client de navigation.
- Les paires Nom/Valeur de type FORM indiquent des informations supplémentaires contenues dans le corps du message des requêtes `POST` HTTP envoyées par le moniteur. Si la page cible contient un formulaire correspondant au nom spécifié dans la zone formname, le moniteur traite toute paire nom/valeur dans le formulaire comme si elle était configurée dans l'élément de profil.

Remarque :

Le moniteur limite la longueur des requêtes HTTP à 4096 caractères. Si la longueur des données de formulaire supplémentaires est à l'origine d'une longueur de demande qui dépasse cette limite, le moniteur n'inclut pas les données de formulaire supplémentaires dans la demande.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur HTTP génère un ensemble de résultats de test contenant les données propres aux tests de service HTTP. Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 77. Eléments du moniteur HTTP

Elément	Description
`$bytesPerSec*(BytesPerSec)`	Nombre moyen d'octets transférés par seconde.
`$bytesTransfered* (BytesTransferred)`	Nombre d'octets transférés ou téléchargés.
`$checksum`	Généralement, l'élément Checksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de total de contrôle ne sont pas connues lorsque l'élément de profil est créé (le moniteur calcule les valeurs de total de contrôle lorsque les tests sont en cours). Les éléments de moniteur $checksum et $previousChecksum sont destinés à l'amélioration des alertes à l'aide du fichier de règles du moniteur.
`$command`	Commande HTTP émise par le moniteur. Par exemple, `HEAD`, `GET`, `GETALL` ou `POST`.
`$connectTime*(ConnectTime)`	Temps mis pour se connecter au serveur.
`$downloadTime*(DownloadTime)`	Temps mis pour télécharger le fichier.
`(Elements)`	Nombre d'éléments de page reçus.
`$formname`	Nom du formulaire utilisé dans une action `POST`.

Tableau 77. Eléments du moniteur HTTP (suite)

Elément	Description
$lastStatus*(PageStatus)	Si un élément de profil extrait plusieurs pages, cet élément contient la chaîne de résultats de la dernière page extraite. Cette valeur est identique à celle de $urlResult*n*, où *n* est égal à la valeur de $pageCount.
$lastModified	Valeur de la zone d'en-tête HTTP Last-Modified de la première page extraite.
$page*(Page)	Page accédée sur le serveur HTTP.
$pageCount	Nombre total de ressources téléchargées pendant un test GETALL, à l'exclusion de la page de test elle-même. Si la page testée ne se rapporte à aucune autre ressource, cet élément n'est pas généré.
$port*(Port)	Port utilisé pour l'accès au serveur HTTP. Si un serveur proxy a été utilisé pour le test, il s'agit de la valeur de port du serveur proxy auquel la demande a été envoyée. Pour préserver le port du serveur de destination prévu, définissez la propriété generateProxyTokens sur 1 ou démarrez le moniteur avec le paramètre de lancement -generateproxytokens.
$previousChecksum	Généralement, l'élément PreviousChecksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de total de contrôle ne sont pas connues quand l'élément de profil est créé (le moniteur calcule les valeurs de total de contrôle lorsque les tests sont en cours). Les éléments de moniteur $previousChecksum et $checksum sont destinés à l'amélioration des alertes à l'aide du fichier de règles du moniteur.
$proxyAuthType	Type d'authentification pour le serveur proxy.
$proxyCache	La valeur true indique que le serveur proxy a extrait la page Web du serveur, plutôt que de son propre cache.
$proxyPort	Numéro de port du serveur proxy auquel la demande a été envoyée.
$proxyServer	Nom d'hôte du serveur proxy.
$proxyUsername	Elément utilisé par le moniteur avec le mot de passe pour établir la connexion au serveur proxy.
$regexpMatch*n*	Contenu de la ligne correspondant à l'expression régulière.
$regexp*n*	Expression régulière.
$regexpMatch*n*	Contenu de la ligne correspondant à l'expression régulière.
$regexpStatus*n*	Etat de la correspondance des expressions régulières : NONE - Aucune vérification d'expression régulière n'est configurée MATCHED - une correspondance a été trouvée pour l'expression régulière FAILED - aucune correspondance n'a été trouvée pour l'expression régulière
$responsetime* (ResponseTime)	Durée entre la création d'une connexion et la réception du premier octet de la page.
$timeSinceModification	Durée écoulée depuis la dernière modification de la page. Il s'agit de la différence entre le moment du test et la valeur de la zone d'en-tête HTTP Last modified de la première page extraite.
$urlDownloadTimes*n** (UrlDownloadTime)	Durée de téléchargement d'URL de chaque élément dans une demande GETALL. Chaque élément est numéroté, à partir de 000 ($urlDownloadTime000, $urlDownloadTime001, $urlDownloadTime002, etc.).
$url*n**(Url)	URL de chaque page d'un test GETALL. Chaque page est numérotée, à partir de 000 ($url000, $url001, $url002, etc.).

Tableau 77. Eléments du moniteur HTTP (suite)

Elément	Description
`$urlResultn*` (`UrlResultString`)	Chaîne de résultat pour chaque page téléchargée dans une demande `GETALL`. Chaque est numéroté, à partir de 000 (`$urlResult000`, `$urlResult001`, `$urlResult002`, etc.).
`$username`	Nom utilisé pour accéder aux pages nécessitant une authentification de l'utilisateur.

Message d'état

Le moniteur HTTP fournit des messages d'état dans l'attribut `ResultMessage` lorsqu'IBM Application Performance Management est utilisé. Ces messages indiquent le résultat du test.

Tableau 78. Tableau 3. Messages d'état du moniteur HTTP

Message	Description
`OK`	La demande émanant du moniteur a abouti.
`Form not found`	La page demandée est introuvable.
`Initialise Fetch Page Failed`	Mémoire insuffisante pour allouer de l'espace au mécanisme d'extraction de la page HTTP. Le message de la ligne précédente doit contenir plus d'informations.
`Connection Failed`	La connexion du moniteur a échoué pour d'autres raisons que la rupture du lien, la réinitialisation de la connexion, l'inaccessibilité du lien, le dépassement du délai de connexion, la fermeture de la connexion ou l'arrêt de l'hôte. Voir le fichier journal du moniteur HTTP pour plus d'informations.

Correspondance des expressions régulières et des paramètres de formulaire

Surveillez le fonctionnement du formulaire `http://support.mycompany.com/cgi-bin/search.cgi` en envoyant des demandes HTTP `POST` avec le paramètre de formulaire `search=ism`, et utilisez une expression régulière pour faire correspondre la chaîne `Your search was successful` dans la réponse. Si cette chaîne est renvoyée dans la réponse, attribuez le niveau de service `Good` et `Failed` dans les autres cas de figure.

Créez un nouvel élément de profil HTTP et définissez les zones comme indiqué dans le tableau ci-dessous.

Tableau 79. Exemple d'élément de profil de formulaire HTTP

Zone de configuration d'élément de profil	Valeur
server	`support.mycompany.com`
page	`/cgi-bin/search.cgi`
description	`Exemple - Expressions régulières et paramètres de formulaire`
Détails sur l'expression régulière	
match 1	`Votre recherche a abouti`
Détails sur la classification de niveau de service	
instruction	`Statut Regexp 1 = CORRESPONDANCE alors statut CORRECT`
Détails sur l'en-tête et le formulaire	
nom	`search`
valeur	`ism`
type	`FORM`

Propriétés

Les propriétés et les options de ligne de commande spécifiques au moniteur HTTP sont décrites dans le tableau suivant.

Tableau 80. Propriétés du moniteur HTTP

Nom de la propriété	Paramètre de la propriété	Description
AllowDuplicateDownload	0|1	Déclenche le téléchargement des pages chaque fois qu'elles sont détectées. 0 - désactivé (un seul téléchargement) 1 - activé
ForceHTMLParse	0|1	Déclenche l'analyse HTML des pages dont le type de contenu n'est pas text/html. 0 - désactivé 1 - activé
GenerateProxyTokens	0|1	Indique si le moniteur génère des éléments supplémentaires contenant des informations sur le serveur proxy si un serveur proxy est utilisé dans un test. 0 - désactivé 1 - activé (les éléments supplémentaires $server et $port contiennent les valeurs du serveur proxy)
GETALLThreadNum	1|2|3|4|5	Spécifie le nombre d'unités d'exécution distinctes à utiliser lors d'une requête GETALL.
GetLinkTags	0|1	Active le téléchargement de feuilles de style liées pour les requêtes GETALL : 0 - désactivé 1 - activé (si la page cible contient une balise link avec la valeur d'attribut rel=stylesheet, le moniteur tente de télécharger la ressource désignée par l'attribut href de la balise link)
HostnameLookupPreference	chaîne	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les valeurs admises sont : • 4Then6 sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • 6Then4 sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • 4Only sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • 6Only sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • 6Or4 sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte. Par défaut : 4Then6

Tableau 80. Propriétés du moniteur HTTP (suite)

Nom de la propriété	Paramètre de la propriété	Description
Ipv6Address	entier	Adresse locale à lier comme origine pour les requêtes HTTP lors de l'utilisation de HTTP IPv6. Par défaut : aucune adresse
NoParseExtensions	chaîne	Liste d'extensions de fichier séparées à l'aide de virgules indiquant les types de fichiers non analysés, mais téléchargés, par le moniteur.
OutputDirectory	chaîne	Indique le répertoire de sortie à utiliser si OutputResult a la valeur true (défini sur 1). Par défaut : $ISHOME/var
OutputResult	0|1	Indique si le moniteur sauvegarde les données qu'il reçoit du service. 0 - désactivé 1 - activé
RelativeRedirects	0|1	Permet aux zones Emplacement des codes d'état HTTP 301/302 de contenir des URL relatives plutôt que des URL absolues. 0 - URL absolues 1 - URL relatives
RFCPOST	0|1	Indique que le moniteur doit suivre les RFC1945 et RFC2616, puis envoyer un deuxième POST après la redirection. De nombreux serveurs Web n'attendent pas un POST après une redirection et la plupart des navigateurs ne suivent pas les RFC. 0 - désactivé 1 - activé

Moniteur HTTPS :

Le moniteur HTTPS vérifie la disponibilité et le temps de réponse des serveurs Web. Il peut surveiller des pages Web individuelles, y compris celles utilisant des formulaires HTML, qui nécessitent normalement que l'utilisateur entre des données dans des zones.

Remarque : Le moniteur HTTPS fonctionne de la même manière que le moniteur HTTP, mais il communique avec le serveur HTTP à l'aide de la version 2 ou 3 du protocole SSL (Secure Sockets Layer), qui chiffre toutes les communications entre le serveur et le moniteur.

Tableau 81. Récapitulatif du fichier de moniteur HTTPS

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	nco_m_https
Fichier de propriétés	$ISHOME/etc/props/https.props
Fichier de règles	$ISHOME/etc/rules/https.rules
Fichier journal	$ISHOME/log/https.log

Consignes de configuration du moniteur HTTPS

Le moniteur HTTPS vérifie la disponibilité et le temps de réponse des serveurs Web. Utilisez le moniteur HTTPS dans les situations suivantes :

- Le site Web cible est statique.

  Pour les sites Web dynamiques, utilisez le moniteur TRANSX.
- Le site Web cible est pris en charge via le protocole HTTPS.

  Pour les sites Web qui fournissent du contenu via le protocole HTTP, sélectionnez le moniteur HTTP.
- Pour effectuer la surveillance sur plusieurs plateformes.
- La vitesse est un facteur déterminant (le moniteur HTTPS offre des performances élevées).

Certificat côté client

Le moniteur permet de surveiller les serveurs qui requièrent des certificats côté client pour une authentification mutuelle.

Spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil.

Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Configuration des tests de service du moniteur HTTPS

Utilisez les paramètres de configuration du moniteur HTTPS pour définir les tests de service HTTPS.

Tableau 82. Configuration du moniteur HTTPS

Zone	Description
serveur	Nom d'hôte du serveur à surveiller. Par exemple : `www.myconpany.com`
page	URL de la page à surveiller. Exemple : `/secure/`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Port du serveur à utiliser. Port par défaut : `443`
localip	Indique l'adresse IP de l'interface réseau utilisée par le moniteur pour le test. Si cette zone est vide, le moniteur utilise l'interface spécifiée par la propriété `IpAddress`.
version	Version du protocole HTTPS à utiliser : • `1.0` • `1.1` Valeur par défaut : `1.0`
command	Type de requête : • `HEAD` • `GET` • `GETALL` • `POST` Valeur par défaut : `GET`

Tableau 82. Configuration du moniteur HTTPS (suite)

Zone	Description
formname	Lorsqu'il est utilisé dans une transaction, le moniteur HTTPS recherche les valeurs par défaut dans le formulaire spécifié. Toutes les valeurs trouvées sont automatiquement remplies dans l'étape HTTPS suivante de la transaction.
authenticationtype	Spécifie le mécanisme d'authentification par stimulation/réponse des utilisateurs réseau : • `NONE` - Aucune authentification. • `BASIC` • `NTLMv1` - Authentification par stimulation/réponse Windows NTLM version 1. • `NTLMv2` - Windows NTLM version 2. Valeur par défaut : `NONE`
username	Nom d'utilisateur (nom de compte) du moniteur à utiliser pour se connecter au serveur HTTPS.
password	Mot de passe correspondant au nom d'utilisateur du moniteur à utiliser pour se connecter au serveur HTTPS.
sslcertificatefile	Chemin d'accès et nom du fichier de certificat numérique qui est utilisé dans l'élément du moniteur. Si le chemin d'accès n'est pas absolu, il est interprété par le moniteur comme étant relatif par rapport au répertoire de travail (`$ISMHOME/platform/arch/bin`). Si vous ne spécifiez pas un fichier de certificat, le moniteur utilise le certificat indiqué par la propriété de moniteur `SSLCertificateFile`.
sslkeyfile	Chemin et nom du fichier contenant la clé privée SSL qui est utilisée pour identifier le serveur et signer les messages SSL.
sslkeypassword	Mot de passe utilisé pour chiffrer la clé privée SSL.
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`
Détails du proxy	
serveur	Nom d'hôte du serveur proxy.
port	Port du serveur proxy à utiliser.
authenticationtype	Type d'authentification pour le serveur proxy HTTPS. Pour plus d'informations, voir authenticationtype.
username	Nom d'utilisateur du moniteur à utiliser pour se connecter au serveur proxy HTTPS.
password	Mot de passe du moniteur à utiliser pour se connecter au serveur proxy HTTPS.

Tableau 82. Configuration du moniteur HTTPS (suite)

Zone	Description
useproxy	Configure le moniteur pour exécuter la demande en utilisant un serveur proxy. • `proxy` (utilisez `true` dans ismbatch) • `noproxy` (utilisez `false` dans ismbatch) Valeur par défaut : `noproxy`
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • `default` définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • `4Then6` sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • `6Then4` sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • `4Only` sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • `6Only` sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • `6Or4` sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur HTTPS tente de faire correspondre les contenus extraits à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations sur la syntaxe des expressions régulières, voir tableau 72, à la page 365.

Paramètre d'en-tête et de formulaire

Comme le moniteur HTTP, le moniteur HTTPS peut envoyer des données supplémentaires dans les zones d'en-tête et le corps du message de requêtes HTTP.

Pour des détails sur les paramètres d'en-être et de formulaire, voir Paramètre d'en-tête et de formulaire HTTP.

Eléments de moniteur

Tableau 83. Eléments du moniteur SSL HTTPS SSL

Elément	Description
`$SSLcertificateSerialNumber`	Numéro de série du certificat X509 présenté par le serveur.

Tableau 83. Eléments du moniteur SSL HTTPS SSL (suite)

Elément	Description
`$SSLcipherSuiteCount`	Nombre d'algorithmes de cryptographie disponibles sur la connexion.
`$SSLcipherSuiteList`	Liste des algorithmes de cryptographie disponibles sur la connexion.
`$SSLcipherSuiteName`	Suite de chiffrement sélectionné pour la connexion.
`$SSLeffectiveSessionKeyBits`	Nombre d'octets dans la clé de session. Il s'agit généralement de `128`, `168`, ou `40` pour les versions d'exportations.

`$SSLHandshakeTime*`
 	
`(SslHandshakeTime)`
	Temps mis pour établir la connexion SSL.

`$SSLissuerName`	Nom d'émetteur pour la certification de format X509 du serveur.
`$SSLprotocolVersion`	Version de SSL utilisée, `v2` ou `v3`.
`$SSLpublicKeyLengthBits`	Taille de la clé publique du serveur. Elle est généralement de `1024` octets, sauf lorsqu'un algorithme de cryptographie de spécification d'exportation est utilisé.
`$SSLserverCertificateValidFrom`	Date de début de validité du certificat du serveur.
`$SSLserverCertificateValidTo`	Date de fin de validité du certificat du serveur.
`$SSLserverName`	Nom du serveur SSL.
`$SSLsubjectName`	Nom de sujet de la certification de format X509. Il s'agit généralement du nom de l'organisation qui contrôle le serveur.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Le moniteur HTTPS produit les mêmes éléments supplémentaires que le moniteur HTTP, comme indiqué dans le tableau 77, à la page 371. En outre, il produit les éléments liés à SSL si un certificat côté client est utilisé dans le test, comme décrit dans le tableau 83, à la page 378.

En plus des résultats de test communs à tous les éléments, le moniteur HTTPS génère un ensemble de résultats de test contenant des données spécifiques aux tests de service HTTPS.

Message de statut

Le moniteur HTTPS fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

En plus des messages d'état HTTP, le moniteur HTTPS génère également les messages répertoriés dans le tableau 84.

Tableau 84. Messages d'état du moniteur HTTPS

Message	Description
`OK`	La connexion du moniteur au serveur a abouti.
`SSL handshake failed`	Le moniteur n'a pas réussi à initialiser la connectivité SSL, une fois la connexion au serveur établie.
`Connection failed`	La connexion du moniteur a échoué pour d'autres raisons que la rupture du lien, la réinitialisation de la connexion, l'inaccessibilité du lien, le dépassement du délai de connexion, la fermeture de la connexion ou l'arrêt de l'hôte. Voir le fichier journal du moniteur HTTP pour plus d'informations.

Propriétés

Le moniteur HTTPS possède les mêmes propriétés que le moniteur HTTP.

Pour plus de détails sur les propriétés et les options de ligne de commande qui sont identiques à celles du moniteur HTTP, voir tableau 80, à la page 374. Le tableau 5 répertorie les propriétés spécifiques de HTTPS.

Tableau 85. Propriétés spécifiques du moniteur HTTPS

Nom de la propriété	Paramètre de la propriété	Description
`SSLCertificate File`	chaîne	Chemin et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément HTTPS lors de sa création. Si le chemin n'est pas absolu, il est interprété par le moniteur comme étant relatif au répertoire de travail (`$ISHOME/platform/arch/bin`).
`SSLCipherSuite`	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Valeur par défaut : `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : `0` - TLSv1 est activé. 1 - TLSv1 est désactivé.
`SSLKeyFile`	chaîne	Fichier contenant la clé privée SSL.
`SSLKeyPassword`	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Algorithmes de chiffrement

La propriété `SSLCipherSuite` spécifie l'algorithme de cryptographie utilisé par le moniteur HTTPS. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 406.

Moniteur IMAP4 :

Le moniteur IMAP4 fonctionne conjointement avec le moniteur SMTP pour tester la disponibilité et le temps de réponse d'un service de messagerie IMAP4.

Le tableau suivant répertorie les fichiers du moniteur IMAP4.

Tableau 86. Fichiers du moniteur IMAP4

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_imap4`
Fichier de propriétés	`$ISHOME/etc/props/imap4.props`
Fichier de règles	`$ISHOME/etc/rules/imap4.rules`
Fichier journal	`$ISHOME/log/imap4.log`

Consignes de configuration du moniteur IMAP4

Le moniteur IMAP4 fonctionne conjointement avec le moniteur SMTP en surveillant la messagerie à laquelle le moniteur SMTP envoie les messages de test et en mesurant le temps nécessaire à la transmission de ces messages.

Remarque : Vérifiez que les horloges système de la machine hôte du moniteur et du serveur de messagerie sont synchronisées afin que le calcul de l'heure de remise fonctionne correctement.

Lorsque le moniteur IMAP4 a lu le contenu de la boîte aux lettres, il génère deux différents types d'événement :

- Evénements propres aux messages

  Le moniteur IMAP4 crée un événement propre aux messages pour chaque message électronique téléchargé à partir de la boîte aux lettres. Dans ce type d'événement, le moniteur attribue à l'élément `$message` la valeur `Message Successfully Downloaded`. L'élément `$timeToDeliver` est calculé en tant que durée nécessaire au transfert du message entre le moniteur SMTP qui l'a émis et la boîte aux lettres qui l'a reçu. L'élément `$hopCount` indique le nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.

- Evénements récapitulatifs

  Le moniteur crée un événement récapitulatif une fois qu'il a traité tous les messages dans la boîte aux lettres. Dans ce type d'événement, l'élément `message` indique le nombre total de messages téléchargés à partir de la boîte aux lettres et l'élément `totaltime` indique la durée nécessaire aux demandes. `$totaltime` est exprimé en secondes.

Messagerie sécurisée

Le moniteur IMAP4 prend en charge les connexions pour la sécurisation des services de messagerie. La connexion peut être effectuée à l'aide de SSL/TLS ou de la commande `STARTTLS`. Lors de la définition d'un élément de profil, utilisez la zone securitytype pour sélectionner la sécurité appropriée. Si le serveur de messagerie requiert un certificat côté client pour le chiffrement SSL, utilisez les propriétés `SSL` pour spécifier un fichier de certificats, un fichier de clés, un mot de passe de clé et une suite de chiffrement.

Certificats client

Le moniteur IMAP4 permet de surveiller les serveurs qui requièrent des certificats côté client pour une authentification mutuelle.

Spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil.

Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Boîtes aux lettres

Une fois que le moniteur IMAP4 a traité les informations se trouvant dans un message électronique envoyé par le moniteur SMTP, il les supprime de la boîte aux lettres. Vous pouvez utiliser une boîte aux lettres existante pour stocker des messages électroniques entre les deux moniteurs même si la boîte aux lettres appartient à un utilisateur réel. Toutefois, il est recommandé de créer un compte de boîte aux lettres spécial pour le test de services.

Configuration des tests de service du moniteur IMAP4

Utilisez les paramètres de configuration du moniteur IMAP4 pour définir les tests de service.

Lorsque vous configurez le moniteur, des valeurs par défaut sont affichées pour les paramètres de délai et d'intervalle d'interrogation. Il s'agit respectivement des valeurs 30 et 300 secondes. D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais appliquées au moment de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Tableau 87. Configuration du moniteur IMAP4

Zone	Description
server	Adresse IP du serveur de messagerie. Par exemple, `test.mycompany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Port IP du serveur IMAP4. Valeur par défaut : `143`
securitytype	Type de connexion sécurisée ouverte avec le serveur de messagerie : • `NONE` - Connexion sans sécurité. • `SSL` - Envoi d'un message `hello` SSLv2, puis négociation SSLv2, SSLv3 ou TLSv1. • `STARTTLS` - Connexion sans sécurité, émission d'une commande `STARTTLS`, puis établissement d'une connexion via TLSv1. Valeur par défaut : `NONE`
username	Nom de boîte aux lettres.
password	Mot de passe utilisé pour se connecter à la boîte aux lettres, le cas échéant.
authenticationtype	Méthode d'authentification à utiliser (`STANDARD` ou `CRAM_MD5`) Valeur par défaut : `STANDARD`
sharedsecret	Secret partagé pour l'authentification CRAM_MD5, le cas échéant.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations sur la syntaxe des expressions régulières, voir tableau 72, à la page 365.

Eléments du moniteur

En plus des résultats de test communs à tous les éléments, le moniteur IMAP4 génère un ensemble de résultats de test contenant des données spécifiques aux tests de service IMAP4.

Le tableau suivant décrit les éléments supplémentaires du moniteur IMAP4.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 88. Eléments du moniteur IMAP4

Elément	Description
`$authentication`	Type de méthode d'authentification requise par le serveur IMAP4 (Standard ou CRAM-MD5).
`$bytesPerSec`	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred`	Nombre d'octets transférés ou téléchargés.
`$connectTime`	Temps mis pour se connecter au serveur IMAP4.
`$downloadTime* (DownloadTime)`	Temps mis pour télécharger le fichier.
`$hopCount`	Nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.
`$inEvent`	Indique que cet événement fait partie d'une série d'événements. `1` indique qu'il ne s'agit pas de l'événement final. `0` indique qu'il s'agit de l'événement final.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$port*(Port)`	Port sur lequel le service est surveillé.
`$responseTime* (ResponseTime)`	Délai entre l'établissement de la connexion et la réception du premier octet de données.
`$security`	Type de connexion sécurisée ouverte avec le serveur de messagerie lors de l'ajout d'un élément IMAP (`NONE`, `STARTTLS` ou `SSL`).
`$sentTo*(SentTo)`	Adresse électronique utilisée par le moniteur SMTP pour envoyer le message d'origine.
`$smtpServer`	Nom du serveur SMTP à partir duquel le message électronique a été envoyé.
`$SSLHandshakeTime* (SslHandshakeTime)`	Temps mis pour établir la connexion SSL.
`$timeToDeliver`	Durée écoulée pour le transfert d'un message électronique entre un moniteur SMTP et la boîte aux lettres de destination.
`$user*(ImapUser)`	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion au serveur IMAP4.

Message d'état

Le moniteur IMAP fournit des messages d'état dans l'attribut `ResultMessage` lorsqu'IBM Application Performance Management est utilisé. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état IMAP4.

Tableau 89. Messages d'état du moniteur IMAP4

Message	Description
`Message successfully downloaded`	Le téléchargement du message a réussi.
`Downloaded x messages`	Indique le nombre de messages dont le téléchargement à partir de la boîte aux lettres a réussi.
`Server not IMAP4rev1 compliant`	Le serveur IMAP4 ne respecte pas la spécification IMAP4 (RFC2060).
`Server does not support STARTTLS capability`	La configuration du serveur n'est pas correcte.
`Unable to log into server`	Le moniteur n'a pas pu se connecter au serveur IMAP.

Tableau 89. Messages d'état du moniteur IMAP4 (suite)

Message	Description
`Unrecognised response to STATUS command`	Le moniteur ne reconnaît pas la valeur renvoyée par le serveur.
`Unrecognised response to FETCH INTERNALDATE command`	
`Failed to obtain Actual-Time-Sent header`	Le moniteur n'a pas obtenu la réponse attendue du serveur.
`Failed to obtain Actually-To header`	
`Failed to obtain SMTP-Server header`	

Propriétés

Les propriétés et les options de ligne de commande spécifiques au moniteur IMAP4 sont décrites dans le tableau suivant.

Tableau 90. Propriétés du moniteur IMAP4

Nom de la propriété	Paramètre de la propriété	Description
`Originator`	chaîne	Spécifie la zone `From` qui doit correspondre lors de la récupération de messages électroniques envoyés par le moniteur SMTP. Le moniteur n'extrait que les messages dont la zone `From` correspond à la chaîne dans Originator (Emetteur). L'Emetteur IMAP4 doit correspondre à l'Emetteur dans le moniteur SMTP. Valeur par défaut : `SMTP-Monitor`
`SSLCertificate File`	chaîne	Chemin d'accès et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément HTTPS lors de sa création. Si le chemin n'est pas absolu, il est interprété par le moniteur comme étant relatif au répertoire de travail (`$ISHOME/platform/arch/bin`).
`SSLCipherSuite`	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Pour une description des valeurs possibles, voir Suites de chiffrement. Valeur par défaut : `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : `0` - TLSv1 est activé. `1` - TLSv1 est désactivé.
`SSLKeyFile`	chaîne	Fichier contenant la clé privée SSL.
`SSLKeyPassword`	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie la suite de chiffrement utilisée par le moniteur IMAP4. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 406.

Moniteur POP3 :

Le moniteur POP3 fonctionne conjointement avec le moniteur SMTP pour tester la disponibilité et le temps de réponse d'un service de messagerie POP3.

Le tableau suivant répertorie les fichiers du moniteur POP3.

Tableau 91. Fichiers du moniteur POP3

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_pop3`
Fichier de propriétés	`$ISHOME/etc/props/pop3.props`
Fichier de règles	`$ISHOME/etc/rules/pop3.rules`
Fichier journal	`$ISHOME/log/pop3.log`

Consignes de configuration du moniteur POP3

Le moniteur POP3 fonctionne conjointement au moniteur SMTP en surveillant la messagerie à laquelle le moniteur SMTP envoie les messages de test et en mesurant la durée nécessaire à la transmission de ces messages.

Remarque : Vérifiez que les horloges système de la machine hôte du moniteur et du serveur de messagerie sont synchronisées afin que le calcul de l'heure de remise fonctionne correctement.

Lorsque le moniteur POP3 a lu le contenu de la boîte aux lettres, il génère deux différents types d'événement :

- Evénements propres aux messages

  Le moniteur POP3 crée un événement propre aux message pour chaque message électronique téléchargé à partir de la boîte aux lettres. Dans ce type d'événement, le moniteur attribue à l'élément `$message` la valeur `Message Successfully Downloaded`. L'élément `$timeToDeliver` est calculé en tant que durée nécessaire au transfert du message entre le moniteur SMTP qui l'a émis et la boîte aux lettres qui l'a reçu. L'élément `$hopCount` indique le nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.
- Evénements récapitulatifs

  Le moniteur crée un événement récapitulatif une fois qu'il a traité tous les messages dans la boîte aux lettres. Dans ce type d'événement, l'élément `message` indique le nombre total de messages téléchargés à partir de la boîte aux lettres et l'élément `totaltime` indique la durée nécessaire aux demandes. `$totaltime` est exprimé en secondes.

Messagerie sécurisée

Le moniteur POP3 prend en charge les connexions pour la sécurisation des services de messagerie. La connexion peut être effectuée à l'aide de SSL/TLS ou de la commande `STARTTLS`. Lors de la définition d'un élément de moniteur POP3, utilisez la zone Type de sécurité pour sélectionner la sécurité appropriée. Si le serveur de messagerie requiert un certificat côté client pour le chiffrement SSL, utilisez les propriétés `SSLname` ou les options de ligne de commande pour spécifier un fichier de certificats, un fichier de clés, un mot de passe de clé et une suite de chiffrement.

Certificat côté client

Le moniteur POP3 permet de surveiller les serveurs qui requièrent des certificats côté client pour une authentification mutuelle. Spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil. Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Configuration des tests du moniteur POP3

Remarque : Surveillez le fonctionnement du serveur de messagerie `mail.mycompany.com` en configurant le moniteur SMTP de telle sorte qu'il envoie des messages à une boîte aux lettres test et en configurant le moniteur POP3 de telle pour l'extraction des messages. L'adresse de la boîte aux lettres est `ismtest@mycompany.com` et ses données d'identification sont `ismtest/secret1`. Utilisez un délai de connexion de 20 secondes, 2 nouvelles tentatives en cas d'échec et un intervalle de cinq secondes, et testez les services toutes les dix minutes. Utilisez les classifications de niveau de service par défaut fournis par les éléments de profil.

Tableau 92. Configuration du moniteur POP3

Zone	Description
server	Adresse IP du serveur de messagerie. Par exemple, `mail.mycompany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Numéro du port du serveur de messagerie. Valeur par défaut : `110`
securitytype	Type de connexion sécurisée ouverte avec le serveur de messagerie : • `NONE` - Connexion sans sécurité • `SSL` - Envoi d'un message `hello` SSLv2, puis négociation SSLv2, SSLv3 ou TLSv1 • `STARTTLS` - Connexion sans sécurité, émission d'une commande `STLS`, puis établissement d'une connexion via TLSv1. Il s'agit du type de sécurité le plus sûr. • `NONE` - Connexion sans sécurité Valeur par défaut : `NONE`
username	Nom de boîte aux lettres.
password	Mot de passe utilisé pour se connecter à la boîte aux lettres, le cas échéant.
authenticationtype	Méthode d'authentification à utiliser et dont le libellé est Type d'authentification : • `STANDARD` - Utilise un échange nom d'utilisateur/mot de passe où le mot de passe n'est pas chiffré. Cette méthode est appropriée pour une utilisation intermittente du protocole POP3. • `APOP` - Utilisez cette méthode quand le client POP3 se connecte régulièrement au serveur. Elle offre un niveau de sécurité plus élevé que la méthode standard. Assurez-vous de spécifier un secret partagé APOP si vous sélectionnez `APOP`. Notez que tous les serveurs ne prennent pas en charge APOP. Valeur par défaut : `STANDARD`.
sharedsecret	Secret partagé pour l'authentification APOP. Applicable uniquement si vous utilisez le type d'authentification APOP. La chaîne doit comporter au moins huit caractères et est masquée dans l'interface utilisateur.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Tableau 92. Configuration du moniteur POP3 (suite)

Zone	Description
verifycertificate	Certificat de vérification du serveur. Valeur par défaut : `Disabled`

Utilisez les paramètres de configuration du moniteur POP3 pour définir les tests de service.

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations sur la syntaxe des expressions régulières, voir tableau 72, à la page 365.

Eléments du moniteur

En plus des résultats de test communs à tous les éléments, le moniteur POP3 génère un ensemble de résultats de test contenant des données spécifiques aux tests de service POP3.

LeTableau 1 décrit les éléments supplémentaires du moniteur POP3.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 93. Eléments du moniteur IMAP4

Elément	Description
`$authentication`	Type de méthode d'authentification requise par le serveur IMAP4 (Standard ou CRAM-MD5).
`$bytesPerSec`	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred`	Nombre d'octets transférés ou téléchargés.
`$connectTime`	Temps mis pour se connecter au serveur IMAP4.
$downloadTime* (`DownloadTime`)	Temps mis pour télécharger le fichier.
`$hopCount`	Nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.
`$inEvent`	Indique que cet événement fait partie d'une série d'événements. 1 indique qu'il ne s'agit pas de l'événement final, `0` indique qu'il s'agit de l'événement final.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$port*(Port)`	Port sur lequel le service est surveillé.
`$responseTime*` (`ResponseTime`)	Délai entre l'établissement de la connexion et la réception du premier octet de données.
`$security`	Type de connexion sécurisée ouverte avec le serveur de messagerie lors de l'ajout d'un élément IMAP (`NONE`, `STARTTLS` ou `SSL`).

Tableau 93. Eléments du moniteur IMAP4 (suite)

Elément	Description
$sentTo*(SentTo)	Adresse électronique utilisée par le moniteur SMTP pour envoyer le message d'origine.
$smtpServer	Nom du serveur SMTP à partir duquel le message électronique a été envoyé.
$SSLHandshakeTime* (SslHandshakeTime)	Temps mis pour établir la connexion SSL.
$timeToDeliver	Durée écoulée pour le transfert d'un message électronique entre un moniteur SMTP et la boîte aux lettres de destination.
$user*(ImapUser)	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion au serveur IMAP4.

Message d'état

Le moniteur POP3 fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau suivant décrit les messages d'état POP3.

Tableau 94. Messages d'état du moniteur POP3

Message	Description
`Message successfully downloaded`	La requête POP3 a abouti.
`Downloaded x messages`	Indique le nombre de messages téléchargés à partir de la boîte aux lettres.
`Timed out waiting to read/write`	Une connexion de données a été établie avec le serveur, mais il a cessé de répondre.
`Connection closed by foreign host`	L'hôte distant a fermé la connexion plus tôt que prévu par le moniteur.
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, reportez-vous au fichier journal.
`APOP not supported by the server`	La méthode d'authentification APOP n'est pas prise en charge par le serveur. Utilisez le type d'authentification Standard à la place.
`APOP service not available`	L'implémentation du serveur APOP n'est pas prise en charge par le moniteur. Utilisez le type d'authentification Standard à la place.
`Server does not support STLS capability`	Le serveur ne prend pas en charge `STARTTLS`. Utilisez un autre type de sécurité.

Propriétés

Les propriétés spécifiques au moniteur POP3 sont décrites dans le tableau suivant.

Tableau 95. Propriétés et options de ligne de commande du moniteur POP3

Nom de la propriété	Paramètre de la propriété	Description
`SSLCertificate File`	chaîne	Chemin et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément POP3 lors de sa création. Si le chemin d'accès n'est pas absolu, il est interprété par le moniteur comme étant relatif par rapport au répertoire de travail (`$ISHOME/platform/arch/bin`).

Tableau 95. Propriétés et options de ligne de commande du moniteur POP3 (suite)

Nom de la propriété	Paramètre de la propriété	Description
SSLCipherSuite	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Valeur par défaut : RC4:3DES:DES:+EXP. Pour une description des valeurs possibles, voir Suites de chiffrement.
SSLDisableTLS	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : 0 - TLSv1 est activé. Définir sur 1 pour désactiver TLSv1.
SSLKeyFile	chaîne	Fichier contenant la clé privée SSL.
SSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Suites de chiffrement

La propriété SSLCipherSuite spécifie la suite de chiffrement utilisée par le moniteur POP3. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 406.

Moniteur ICMP :

Le moniteur ICMP teste les performances du service ICMP exécuté sur un réseau. Pour ce faire, le moniteur utilise la commande écho ICMP.

Le tableau ci-dessous répertorie les fichiers du moniteur ICMP.

Tableau 96. Fichiers du moniteur ICMP

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	nco_m_icmp
Fichier de propriétés	$ISHOME/etc/props/icmp.props
Fichier de règles	$ISHOME/etc/rules/icmp.rules
Fichier journal	$ISHOME/log/icmp.log

Instructions de configuration du moniteur ICMP

Le moniteur ICMP envoie des demandes d'écho ICMP (généralement appelées pings) aux hôtes cible et attend des réponses d'écho. Il enregistre les temps de réponse, les durées de boucle et les mesures de taux de réussite qui fournissent une indication du fonctionnement du réseau. Lorsque le moniteur émet une demande d'écho, la demande peut passer par un ou plusieurs routeurs avant d'atteindre l'hôte cible. Ces routeurs peuvent répondre au moniteur avant que l'hôte cible ait reçu la demande d'écho. Si une demande d'écho émise par le moniteur passe par un routeur, ce routeur peut émettre une réponse destinée au moniteur. Cette réponse peut indiquer que le routeur n'a pas pu définir l'emplacement de l'hôte cible ou que le routeur est trop occupé pour traiter la demande. Il est possible que le moniteur reçoive des réponses de plusieurs routeurs avant qu'il ne reçoive une réponse d'écho de l'hôte cible. Si le moniteur reçoit une réponse d'écho de l'hôte cible, il enregistre la durée. S'il ne reçoit pas de réponse du serveur cible pendant la période définie, la demande est enregistrée comme un échec. Vous pouvez configurer le moniteur afin qu'il envoie plusieurs demandes d'écho ICMP vers la même cible dans chaque test. Le moniteur enregistre les statistiques de chaque demande envoyée.

Remarque : Le moniteur ICMP doit être exécuté en tant que superutilisateur root car il ouvre un socket brut pour envoyer des paquets ICMP.

Configuration des tests d'un service du moniteur ICMP

Utilisez les paramètres de configuration du moniteur ICMP pour définir les tests d'un service. Lorsque vous configurez le moniteur, des valeurs par défaut sont affichées pour les paramètres de délai et d'intervalle d'interrogation. Il s'agit respectivement des valeurs 30 et 300 secondes. D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais appliquées au moment de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Le tableau suivant répertorie les configurations du moniteur ICMP.

Tableau 97. Configuration du moniteur ICMP

Zone	Description
serveur	Nom d'hôte ou adresse IP du serveur auquel les demandes d'écho sont envoyées. Par exemple, `test.myconpany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
timeout	Délai d'attente, en secondes, d'une réponse du serveur à chaque demande d'écho. Valeur par défaut : `10`
numberofpings	Nombre de demandes d'écho à envoyer. Valeur par défaut : `5`
packetinterval	Délai d'attente, en secondes, entre l'envoi de demandes d'écho. Valeur par défaut : `1`
packetsize	Taille, en octets, de chaque demande d'écho envoyée. Valeur par défaut : `64`
typeofservice	Définit la zone Type of Service dans la couche IP. Les valeurs des zones TOS (Type of Service) IPv4 et DSCP Differentiated Service doivent être entrées. Les valeurs admises sont comprises entre `0` et `255`.
retries	Nombre de nouvelles tentatives du moniteur pour effectuer des demandes d'écho avant d'abandonner la procédure. Valeur par défaut : `0`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Tableau 97. Configuration du moniteur ICMP (suite)

Zone	Description
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • `default` définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • `4Then6` sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • `6Then4` sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • `4Only` sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • `6Only` sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • `6Or4` sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.

Remarque : Surveillez la disponibilité de l'hôte `test.mycompany.com` en vérifiant les temps de réponse toutes les dix minutes. Tentez d'établir une connexion au serveur dans un intervalle de 30 secondes et si le délai est dépassé, faites deux nouvelles tentatives. Si ces tentatives n'aboutissent pas, répétez le test trois fois avec cinq secondes entre chaque tentative.

Eléments du moniteur

En plus des résultats de test communs à tous les éléments, le moniteur ICMP génère un ensemble de résultats de test contenant des données propres aux tests du service ICMP.

Le tableau ci-dessous décrit les éléments supplémentaires du moniteur ICMP.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 98. Eléments du moniteur ICMP

Elément	Description
`$averageRTT*(AverageRTT)`	Durée moyenne de la boucle, en secondes.
`$endTime`	Heure UNIX à laquelle la réponse a été reçue.
`$jitter`	Valeur absolue de la différence entre les heures d'arrivée de deux demandes d'écho ICMP adjacentes, moins leurs heures de départ. Cette valeur est calculée conformément à la formule spécifiée dans RFC2598. L'élément est créé uniquement si le nombre de demandes d'écho est supérieur à 1. Si plus de deux demandes d'écho sont utilisées, la valeur correspond à la gigue moyenne entre toutes les paires de demandes d'écho.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$maxRTT*(MaxRTT)`	Durée maximale de la boucle, en secondes.
`$minRTT*` `(MinRTT)`	Durée minimale de la boucle, en secondes.
`$numberPackets`	Nombre de demandes d'écho ICMP envoyées, comme indiqué dans l'élément de profil.

Tableau 98. Eléments du moniteur ICMP (suite)

Elément	Description
$packetInterval	Temps d'attente entre l'envoi de chaque demande d'écho ICMP, comme indiqué dans l'élément de profil.
$packetRetries	Nombre de nouvelles tentatives effectuées par le moniteur pour renvoyer des demandes d'écho ICMP avant d'abandonner la procédure.
$packetSize	Taille (en octets) de chaque demande d'écho ICMP, comme indiqué dans l'élément de profil.
$pingAttempts Failed	Nombre de tentatives effectuées pour la première demande d'écho ICMP qui a échoué.
$pingAttempts Responded	Nombre de tentatives effectuées pour la première demande d'écho ICMP réussie.
$pingMessageFailed	Message renvoyé pour la première demande d'écho ICMP ayant échoué.
$pingMessage Responded	Message renvoyé pour la première demande d'écho ICMP réussie.
$pingReceivedTime Failed	Heure UNIX à laquelle la première réponse d'échec de l'écho a été reçue.
$pingReceivedTime Responded	Heure UNIX à laquelle la première réponse de réussite de l'écho a été reçue.
$pingRespondIP Failed	Adresse IP qui a répondu à la première demande d'écho ICMP ayant échoué.
$pingRespondIP Responded	Adresse IP qui a répondu à la première demande d'écho ICMP réussie.
$pingRTTFailed	Durée de la boucle de la première demande d'écho ICMP ayant échoué, en secondes.
$pingRTTResponded	Durée de la boucle de la première demande d'écho ICMP réussie, en secondes.
$pingSentTime Failed	Heure UNIX à laquelle la première demande d'écho ICMP ayant échoué à été envoyée.
$pingSentTime Responded	Heure UNIX à laquelle la première demande d'écho ICMP réussie a été envoyée.
$pingsFailed	Nombre de demandes d'écho ICMP envoyées pour lesquelles il n'y a eu aucune réponse d'écho.
$pingsResponded	Nombre de réponses d'écho valides reçues.
$pingTime	Temps mis pour recevoir la réponse d'écho après l'envoi de la demande d'écho ICMP.
$respondPercent* (RespondPercent)	Pourcentage de demandes d'écho ICMP envoyées pour lesquelles il y a eu une réponse.
$responseTime	Temps mis pour que l'hôte cible réponde à une demande d'écho ICMP.
$sentTime	Heure UNIX à laquelle les demandes d'écho ICMP ont été envoyées.
$spreadRTT	Différence entre $maxRTT et $minRTT.
$startTime	Heure UNIX de début du test.
$totalHostTime	Temps mis pour recevoir la réponse d'écho après le début du test.
$typeOfService	Zone Type of Service de la couche IP, comme spécifié lors de l'ajout d'un nouvel élément ICMP. Pour plus d'informations, voir «Moniteur ICMP», à la page 389.

Le moniteur ICMP crée un ensemble distinct d'éléments $pingname pour enregistrer les résultats de chaque demande d'écho ICMP envoyée pendant le test. Le nombre de demandes envoyées est indiqué par $numberPackets. Par exemple, pour l'élément $pingRTT, si $numberPackets correspond à 3, le moniteur crée trois éléments ($pingRTT1, $pingRTT2 et $pingRTT3), qui contiennent les mesures de durée de la boucle des trois demandes d'écho ICMP envoyées.

Message d'état

Le moniteur ICMP fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état ICMP.

Tableau 99. Messages d'état du moniteur ICMP

Message	Description
`Pings Complete`	La demande d'écho ICMP a abouti.
`ICMP echo failed`	Le moniteur n'a pas pu émettre la demande d'écho ICMP en raison d'un problème avec l'hôte du moniteur ou avec sa connexion au réseau.
`Timed out`	La demande d'écho ICMP a dépassé le délai d'attente.
`Inaccessible`	Ce message est renvoyé par un routeur et n'est pas nécessairement correct.
`Source quench`	Un routeur est trop occupé pour traiter la demande d'écho ICMP.
`Time exceeded`	Ce message est renvoyé par un routeur. Il indique que la demande d'écho ICMP à été acheminée sur le réseau trop de fois.
`Parameter problem`	Ce message est renvoyé par un routeur. Il indique que le routeur ne peut pas traiter la demande d'écho ICMP. La cause peut être l'altération du message.

Propriétés

Les propriétés propres au moniteur ICMP sont décrites dans le tableau ci-dessous.

Tableau 100. Propriétés ICMP

Nom de la propriété	Paramètre de la propriété	Description
`EventsPerSec`	non applicable	Cette propriété n'est pas prise en charge.
`IntraPingWait`	entier	L'intervalle de temps minimum, en millisecondes, entre toutes les commandes ping envoyées par le moniteur ICMP. Utilisez-le pour régler les paramètres de votre système afin de répartir le trafic réseau sur une période plus importante. Par exemple, dans un environnement comportant des milliers d'hôtes ICMP ciblés, affectez la valeur `3` à `IntraPingWait`. Valeur par défaut : `0`
`Ipv6Address`	entier	Adresse locale à lier comme origine pour les demandes d'écho ICMP lors de l'utilisation d'ICMP IPv6. Par défaut : aucune adresse
`MaxDNSResolvingThreads`	entier	Nombre maximal d'unités d'exécution qui doivent être utilisées par le programme de résolution DNS. Valeur par défaut : `20`
`MaxPacketSize`	entier	Taille maximale du paquet ICMP en octets.
`PingsPerSec`	entier	Nombre de demandes d'écho que le moniteur tente d'envoyer par seconde. Le nombre de demandes réellement envoyées dépend de la charge de l'unité centrale et du réseau. Valeur par défaut : `100`
`SocketBufferSize`	entier	Taille de la mémoire tampon du socket de réception (en kilooctets). Valeur par défaut : `32`

Moniteur TCPPort :

Le moniteur TCPPort fournit une couverture des services non testés par les autres moniteurs. Il détecte les commandes ou les chaînes d'un port TCP et y répond. Ce moniteur est particulièrement utile pour surveiller les services indiqués.

Le tableau suivant répertorie les fichiers du moniteur TCPPort.

Tableau 101. Fichiers du moniteur TCPPort

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_tcpport`
Fichier de propriétés	`$ISHOME/etc/props/tcpport.props`
Fichier de règles	`$ISHOME/etc/rules/tcpport.rules`
Fichier journal	`$ISHOME/log/tcpport.log`

Consignes de configuration du moniteur TCPPort

Le moniteur TCPPort teste les services de type TCP en établissant une connexion au service, en surveillant les messages reçus du service et en lui envoyant des réponses.

Pour configurer un test, définissez une séquence de messages et de réponses attendus qui se compose d'une interaction normale sur ce service.

Par exemple, une interaction standard d'un service telnet implique la séquence suivante :

1. Le service telnet envoie un message de connexion, vous invitant à entrer un nom d'utilisateur.
2. Le client envoie une réponse contenant un nom d'utilisateur.
3. Le service telnet envoie un message, vous invitant à entrer un mot de passe.
4. Le client envoie une réponse contenant un mot de passe.
5. Si la tentative de connexion aboutit, le service telnet envoie un message de bienvenue.

Les propriétés `WaitForn` et `Sendn` du moniteur définissent les messages attendus et les réponses à ces messages. Ces propriétés, définies dans le fichier de propriétés du moniteur, définissent le mode d'interaction du moniteur avec le service TCP :

- Les propriétés `WaitForn` sont des expressions régulières. Le moniteur les utilise pour la correspondance des messages reçus sur le port surveillé.
- Les propriétés `Sendn` sont des chaînes littérales que le moniteur écrit sur le port.

Remarque : Si nécessaire, vous pouvez insérer des caractères de contrôle dans ces propriétés à l'aide d'un éditeur de texte qui prend en charge l'insertion de caractères de contrôle.

Le format permettant de définir les propriétés `WaitForn` et `Sendn` est :

WaitFor1 : 1er message reçu

WaitFor2 : 2ème message reçu

Send1 : 1ère réponse

Send2 : 2ème réponse

...

WaitFor5 : 5ème message reçu

Send5 : 5ème réponse

Lorsque le moniteur atteint la première propriété `WaitFor` non définie, il arrête les opérations d'envoi et de réception. Si la propriété `MonitorDisconnect` a la valeur `0`, le service surveillé doit fermer la connexion ouverte par le moniteur. Sinon, le moniteur inclut un message indiquant que

le délai a expiré lors de l'attente de la lecture (`Timed out waiting to read`) dans son élément `$message`. Avec un grand nombre de services, vous pouvez fermer la connexion en envoyant une commande `quit`. Si `MonitorDisconnect` a la valeur 1, le moniteur se déconnecte à la fin de la dernière commande `Send` ou `WaitFor` ou une fois que le délai est atteint.

Configuration du test de service du moniteur TCPPort

Utilisez les paramètres de configuration du moniteur TCPPort pour définir les tests de service.

Tableau 102. Configuration de TCPPort

Zone	Description
serveur	Adresse IP de la machine sur laquelle le service cible est en cours d'exécution. Par exemple, `server.mycompany.com`
port	Port sur lequel se connecter au service cible.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
délai d'attente	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Remarque : Surveillez la disponibilité du service `telnet` en cours d'exécution sur l'hôte `server.mycompany.com` sur le port 23. Utilisez les données d'identification `user` ou `guest` pour vous connecter au serveur et fermez la connexion immédiatement après la connexion établie. Exécutez le test toutes les 5 minutes et définissez un délai d'attente de 10 secondes pour les tentatives de connexion.

1. Ajoutez les entrées suivantes dans le fichier de propriétés TCPPort :

```
WaitFor1: ".*[Ll]ogin:"
Send1: "user"
WaitFor2: ".*[Pp]assword:"
Send2: "guest"
WaitFor3: ".*%"
Send3: "exit"
```

2. Démarrez ou redémarrez le moniteur TCPPort.

Correspondances d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur TCPPort tente de faire correspondre les contenus extraits à chaque expression régulière. Si une correspondance à une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations sur la syntaxe des expressions régulières, voir tableau 72, à la page 365.

Eléments du moniteur

Le tableau suivant décrit les éléments supplémentaires du moniteur TCPPort.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

En plus des résultats de test communs à tous les éléments, le moniteur TCPPort génère un ensemble de résultats de test contenant des données spécifiques aux tests de service TCPPort.

Tableau 103. Eléments du moniteur TCPPort

Elément	Description
`$bytesPerSec`	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred`	Nombre d'octets transférés ou téléchargés.
`$connectTime*(ConnectTime)`	Temps mis pour établir une connexion au serveur cible.
`$downloadTime*(DownloadTime)`	Temps mis pour télécharger des données.
`$lastlineThere's`	Contenus de la dernière ligne reçue du serveur cible.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$networkError`	Contient toutes les erreurs réseau survenues pendant la connexion.
`$port*` `(Port)`	Port du serveur cible auquel le moniteur a tenté de se connecter.
`$waitingFor`	Si la connexion est arrêtée avant que le moniteur n'ait terminé sa séquence d'attentes et d'envois, cet élément contient les contenus de la dernière propriété `WaitFor`.

Message d'état

Le moniteur TCPPort fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau suivant décrit les messages d'état TCPPort.

Tableau 104. Messages d'état du moniteur TCPPort

Message	Description
`OK`	Demande effectuée.
`Timed out waiting to read/write`	Une connexion de données a été établie avec le serveur, mais il a cessé de répondre.
`Connection closed unexpectedly`	La connexion au serveur a été interrompue.
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, reportez-vous au fichier journal.
`Network connect error`	Un incident a été détecté sur le réseau.
`Network error whilst reading`	

Propriétés

Les propriétés spécifiques au moniteur TCPPort sont décrites dans le tableau suivant.

Tableau 105. Propriétés du moniteur TCPPort

Nom de la propriété	Paramètre de la propriété	Description
`Monitor Disconnect`	`0`|`1`	Indique que le moniteur doit se déconnecter après la dernière commande `Send` ou `WaitFor`. Si la dernière commande est `Send`, le moniteur se déconnecte immédiatement après l'envoi de la chaîne. Si la dernière commande est `WaitFor`, le moniteur se déconnecte dès qu'il reçoit une correspondance ou lorsque le délai d'attente de l'interrogation est dépassé. `0` - désactivé (le moniteur ne se connecte pas) `1` - activé
`OutputDirectory`	chaîne	Indique le répertoire de sortie à utiliser si `OutputResult` est sauvegardé. Valeur par défaut : `$ISHOME/var`.
`OutputResult`	`0`|`1`	Indique que le moniteur doit sauvegarder les données qu'il reçoit du service. `0` - désactivé `1` - activé
`Send`	*n*	Chaîne littérale que le moniteur écrit sur le port. Voir Consignes de configuration du moniteur TCPPort. `n` est une valeur numérique comprise entre 1 et 3 (incluse).
`singleLineMatch`	`0`|`1`	Indique que le moniteur renvoie une seule correspondance de ligne en cas de correspondance à une expression régulière. `0` - désactivé (plusieurs lignes sont recherchées) `1` - activé (une seule ligne est recherchée)
`WaitFor`	*n*	Expression régulière utilisée pour faire correspondre les commandes ou chaînes sur le port surveillé. Pour plus d'informations sur cette propriété, voir Consignes de configuration du moniteur TCPPort. `n` est une valeur numérique comprise entre 1 et 30 (incluse).

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie la suite de chiffrement utilisée par le moniteur TCPPORT. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 406.

Moniteur SMTP :

Le moniteur SMTP fonctionne conjointement avec les moniteurs IMAP4 ou POP3 pour tester les performances d'un service de messagerie.

Le tableau suivant répertorie les fichiers du moniteur SMTP.

Tableau 106. Fichiers du moniteur SMTP

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_smtp`
Fichier de propriétés	`$ISHOME/etc/props/smtp.props`

Tableau 106. Fichiers du moniteur SMTP (suite)

Fichiers du moniteur	Nom ou emplacement
Fichier de règles	`$ISHOME/etc/rules/smtp.rules`
Fichier journal	`$ISHOME/log/smtp.log`

Consignes de surveillance du moniteur SMTP

Le moniteur SMTP fonctionne conjointement avec les moniteurs POP3 ou IMAP4. Il envoie régulièrement un message électronique à une boîte aux lettres sur le serveur cible et enregistre la durée nécessaire à l'émission d'une demande de courrier électronique. Le moniteur POP3 ou IMAP4 lit ensuite les messages dans la boîte aux lettres et les utilise pour calculer le temps de réponse et la disponibilité du service de messagerie électronique.

Remarque : Le moniteur SMTP fonctionne conjointement avec les moniteurs POP3 ou IMAP4. Il envoie régulièrement un message électronique à une boîte aux lettres sur le serveur cible et enregistre la durée nécessaire à l'émission d'une demande de courrier électronique. Le moniteur POP3 ou IMAP4 lit ensuite les messages dans la boîte aux lettres et les utilise pour calculer le temps de réponse et la disponibilité du service de messagerie électronique.

Boîtes aux lettres

Vous pouvez configurer le moniteur afin qu'il envoie des messages électroniques à une boîte aux lettres existante même si la boîte aux lettres appartient à un utilisateur réel. Toutefois, il est recommandé de créer un compte de boîte aux lettres spécial pour le test de services. Le paramètre de messagerie indique la boîte aux lettres du destinataire. Par défaut, le moniteur envoie des messages de test avec la ligne d'objet `SMTP Monitor Test Message`. Le cas échéant, vous pouvez configurer des éléments de profil SMTP avec un nom de boîte aux lettres. Dans cette configuration, le moniteur vérifie tout simplement que le service SMTP accepte les connexions.

Messageries sécurisées

Le moniteur SMTP prend en charge les connexions pour la sécurisation des services de messagerie. La connexion peut être effectuée à l'aide de SSL/TLS ou de la commande `STARTTLS`. Lors de la définition d'un élément de moniteur SMTP, utilisez la zone Security Type pour sélectionner la sécurité appropriée. Si le serveur de messagerie requiert un certificat côté client pour le chiffrement SSL, utilisez les propriétés `SSLname` ou les options de ligne de commande pour spécifier un fichier de certificats, un fichier de clés, un mot de passe de clé et une suite de chiffrement.

Certificat côté client

Le moniteur SMTP vous permet de surveiller des serveurs qui requièrent des certificats côté client pour l'authentification mutuelle. Vous spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil. Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Configuration des tests de service du moniteur SMTP

Utilisez les paramètres de configuration du moniteur SMTP pour définir les tests de service. Lorsque vous configurez le moniteur, des valeurs par défaut sont affichées pour les paramètres de délai et d'intervalle d'interrogation. Il s'agit respectivement des valeurs 30 et 300 secondes.

D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais appliquées au moment de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Tableau 107. Configuration du moniteur SMTP

Zone	Description
server	Adresse IP du serveur de messagerie. Par exemple : `mail.mycompany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Numéro du port du serveur de messagerie. Valeur par défaut : `25` Si vous utilisez un autre serveur que le serveur SMTP, mettez à jour son port de connexion. Par exemple, si vous utilisez un serveur IMAP4 via SSL for Microsoft Exchange, spécifiez le port 465.
securitytype	Type de connexion sécurisée ouverte avec le serveur de messagerie : • `NONE` - Connexion sans sécurité • `SSL` - Envoi d'un message `hello` SSLv2, puis négociation SSLv2, SSLv3 ou TLSv1 • `STARTTLS` - Connexion sans sécurité, émission d'une commande `STARTTLS`, puis établissement d'une connexion via TLSv1 Valeur par défaut : `NONE`
username	Nom d'utilisateur utilisé pour se connecter au serveur SMTP. Utilisé avec l'authentification `PLAIN` ou `CRAM-MD5`.
password	Mot de passe utilisé pour se connecter au serveur SMTP. Utilisé avec l'authentification `PLAIN` ou `CRAM-MD5`.
authenticationtype	Méthode d'authentification du moniteur sur le serveur SMTP. Les options disponibles sont les suivantes : • `NONE` - Aucune tentative d'authentification • `PLAIN` - Authentification du nom d'utilisateur et du mot de passe en clair • `CRAM-MD5`- L'authentification CRAM-MD5 est utilisée La valeur par défaut est `NONE`.
sharedsecret	Clé secrète partagée pour l'authentification CRAM-MD5.
email	Adresse électronique de la boîte aux lettres utilisée par les moniteurs SMTP et POP3.
timeout	Délai d'attente, en secondes, d'une réponse du serveur SMTP. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Remarque : Surveillez la disponibilité du serveur de messagerie `mail.mycompany.com` en tentant d'y établir une connexion toutes les dix minutes. Utilisez un délai de connexion de trente secondes et si cette tentative n'aboutit pas, faites trois nouvelles tentatives avec cinq secondes entre chaque tentative.

Elément de moniteur

En plus des résultats de test communs à tous les éléments, le moniteur SMTP génère un ensemble de résultats de test contenant des données spécifiques aux tests de service SMTP.

Le tableau suivant décrit les éléments supplémentaires pour le moniteur SMTP.

Tableau 108. Eléments de moniteur SMTP

Elément	Description
`$authentication`	Type de méthode d'authentification utilisateur requis par le serveur SMTP (`Standard` ou `APOP`).
`$bytesPerSec`	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred`	Nombre d'octets transférés ou téléchargés.
`$connectTime*` `(ConnectTime)`	Temps mis pour se connecter au serveur SMTP.
`$email*` `(EmailAddress)`	Adresse électronique de la boîte aux lettres à laquelle le moniteur envoie un courrier électronique de test.
`$lookupTime*` `(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$port*` `(Port)`	Port sur lequel le service est surveillé.
`$responseTime*` `(ResponseTime)`	Durée entre la création d'une connexion et l'envoi du premier octet du message test au serveur SMTP.
`$security`	Type de connexion sécurisée ouverte avec le serveur de messagerie (`NONE`, `STARTTLS` ou `SSL`), défini dans la zone **type_sécurité** de l'élément de profil.
`$SSLHandshakeTime*` `(SslHandshakeTime)`	Temps mis pour établir la connexion SSL.
`$status*` `(ResultStatus)`	Code d'état renvoyé par le serveur SMTP.
`$uploadTime*` `(UploadTime)`	Temps mis pour charger le fichier.
`$user*` `(SmtpUser)`	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion au serveur SMTP.

Message d'état

Le moniteur SMTP fournit des messages d'état dans l'élément `$message` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Propriétés

Les propriétés spécifiques du moniteur SMTP sont décrites dans le tableau suivant.

Tableau 109. Propriétés et options de ligne de commande du moniteur SMTP

Nom de la propriété	Paramètre de la propriété	Description
`MailMessage Path`	chaîne	Chemin d'accès à un fichier contenant le texte à envoyer dans le courrier électronique de test. Un message par défaut est envoyé si cette propriété n'est pas définie.
`Originator`	chaîne	Spécifie la zone `From` à définir lors de l'envoi d'un courrier électronique de test. Assurez-vous qu'elle corresponde à la chaîne équivalente du moniteur IMAP4. Valeur par défaut : `SMTP-Monitor`
`SSLCertificate File`	chaîne	Chemin et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément SMTP lors de sa création. Si le chemin n'est pas absolu, il est interprété par le moniteur comme étant relatif au répertoire de travail (`$ISHOME/platform/arch/bin`).
`SSLCipherSuite`	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Pour une description des valeurs possibles, voir Algorithmes de cryptographie. Valeur par défaut : `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : `0` - TLSv1 est activé. 1 TLSv1 est désactivé.
`SSLKeyFile`	chaîne	Fichier contenant la clé privée SSL.
`SSLKeyPassword`	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.
`UseBody`	entier	Indique l'endroit où le moniteur écrit les informations de suivi dans le courrier électronique (en-tête ou corps de texte). Par défaut : `0` - les informations sont incluses dans l'en-tête du courrier électronique. `1` - consigne des informations dans le corps du message.

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie l'algorithme de cryptographie utilisé par le moniteur SMTP. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 406.

Moniteur TRANSX :

Le moniteur TRANSX simule les actions d'un utilisateur Internet réel en exécutant une série d'activités à l'aide d'autres moniteurs de service Internet.

Par exemple, vous pouvez configurer TRANSX pour accéder à des pages d'un site Web à l'aide du moniteur HTTP, télécharger certains fichiers, envoyer ou extraire des e-mails à l'aide des moniteurs POP3 et SMTP.

Le tableau ci-dessous répertorie les fichiers du moniteur TRANSX.

Tableau 110. Fichiers du moniteur TRANSX

Fichiers du moniteur	Nom ou emplacement
Exécutable du moniteur	`nco_m_transaction`
Fichier de propriétés	`$ISHOME/etc/props/transx.props`

Tableau 110. Fichiers du moniteur TRANSX (suite)

Fichiers du moniteur	Nom ou emplacement
Fichier de règles	`$ISHOME/etc/rules/transx.rules`
Fichier journal	`$ISHOME/log/transx.log`

Propriétés

Tableau 111. Propriétés du moniteur TRANSX

Nom de la propriété	Paramètre de la propriété	Description
`CompleteTransax`	`0`|`1`	Indique que la transaction continue même en cas d'échec d'une étape. • `0` - désactivé (ne continue pas) • `1` - activé (continue)
`DetailedTimings`	`0`|`1`	Indique que le moniteur TRANSX produit des fichiers datalog contenant des durées à granularité fine pour chaque étape. Les durées à granularité fine produites dans les fichiers datalog sont prédéfinies et ne peuvent pas être modifiées. • `0` - désactivé • `1` - activé
`MultipleEvents`	`0`|`1`	Indique si le moniteur génère plusieurs événements pour les résultats de transaction : • `0` - désactivé (le moniteur génère un seul événement contenant les résultats de toutes les étapes et les résultats récapitulatifs) • `1` - activé (le moniteur génère un événement pour chaque étape de transaction, ainsi qu'un événement récapitulatif final)
`StepPause`	entier	Indique la durée de la pause, en secondes, entre l'exécution de chaque étape de la transaction. La durée de la pause n'affecte pas la valeur de l'élément `$totalTime` d'une transaction. `$totalTime` représente la somme des éléments `$stepXTime` d'une transaction. Valeur par défaut : `0`

Le tableau ci-dessous décrit les propriétés propres au moniteur SMTP.

Consignes de configuration du moniteur TRANSX

Le moniteur TRANSX teste des services en simulant un ensemble d'activités qui impliquent une expérience utilisateur standard. L'ensemble d'activités est appelé une `transaction`, et chaque activité de la transaction est appelée une `étape de transaction`.

Les éléments de profil TRANSX définissent les transactions. Chaque étape de transaction configure un moniteur de service Internet, comme un moniteur HTTP, pour exécuter l'opération pour cette étape. Vous configurez les étapes de transaction à l'aide du bouton Editer dans l'onglet Etapes de l'élément de profil TRANSX.

Les étapes sont configurées de la même manière que tout autre élément de profil. Par exemple, les détails de configuration d'une étape qui implique le moniteur HTTP peuvent inclure des paramètres d'en-tête/formulaire, des paramètres de serveur proxy, des expressions régulières et des classifications de niveau de service.

Lorsque le moniteur TRANSX teste une étape dans la transaction, il enregistre la durée et le niveau de service de l'étape.

Remarque : Le moniteur TRANSX requiert des droits d'accès de niveau superutilisateur si des étapes de transaction utilisent un autre moniteur, ICMP par exemple, qui requiert ces droits d'accès.

Gestion du contenu dynamique avec des moniteurs HTTP et HTTPS

Un grand nombre de sites Web utilisent un contenu dynamique pour fournir des fonctions, telles des interactions basées sur des régions ou des sessions. En cas d'utilisation avec le moniteur TRANSX, les moniteurs HTTP et HTTPS peuvent tester les pages Web qui contiennent du contenu dynamiques, comme des ID session, des codes de région ou des dates et des heures intégrés dans des liens, dont les valeurs peuvent être différentes à chaque test de la transaction.

Les fonctions de contenu dynamique fournies par les moniteurs HTTP et HTTPS lors de l'exécution en mode transaction permettent d'identifier le contenu dynamique sous la forme de paires nom-valeur, appelées `éléments de page dynamique`, intégrées dans des URL ou définies dans des éléments `form` HTML, que le moniteur extrait ensuite d'une page lors de chaque test, garantissant que la valeur dynamique appropriée est utilisée à chaque test d'une transaction.

Par exemple, prenons en compte une page de connexion d'un site Web, `http://www.mycompany.com/login`, qui contient un lien permettant de se connecter au site Web. L'URL de lien de l'action de connexion `http://www.mycompany.com/doLogin?sessionID=id` inclut un ID session pour la transaction de connexion. Dans cet exemple, la paire nom-valeur est un élément de page dynamique `sessionID=id` ; la valeur `id` change à chaque accès de la page de connexion. Si vous souhaitez tester la page de connexion dans le cadre d'une transaction, configurez la transaction pour obtenir et utiliser la valeur de `sessionID` à chaque test de la transaction et l'insérer dans l'URL d'action de connexion.

Le moniteur TRANSX fait passer des éléments de page dynamique d'une étape de transaction à la suivante. Dans l'exemple de connexion au site Web, la première étape de la transaction accède à la page de connexion pour obtenir l'ID session, puis le transmet à une deuxième étape qui soumet la demande de connexion contenant cet ID. Les opérations effectuées dans ces étapes sont les suivantes :

1. Accès à la page contenant les éléments de page dynamique, par exemple `http://www.mycompany.com/login`
2. Soumission de l'action utilisant les éléments de page dynamique, par exemple `http://www.mycompany.com/doLogin?sessionID=@@030671`

Lorsque vous identifiez un élément de page dynamique dans une étape de transaction, il est transmis à la prochaine étape de transaction qui insère la paire nom-valeur dans sa demande. L'élément est transmis à chaque transaction HTTP ou HTTPS suivante jusqu'à ce que vous la supprimiez explicitement.

Ajout et suppression des pages dynamiques

Chaque étape de transaction HTTP ou HTTPS est constituée d'une demande, qui renvoie une page HTML. Lors de l'exécution d'une étape de transaction qui contient des éléments de page dynamiques, le moniteur analyse la page HTML pour définir l'emplacement de chaque paire nom-valeur d'élément et le transmet à l'étape de transaction suivante, qui les insère dans la requête HTTP ou HTTPS.Pour indiquer qu'une étape utilise des éléments de page dynamiques, associez le type de paramètre de l'élément à la valeur DYNAMIC. Indiquez ensuite chaque élément dynamique à extraire et passez aux étapes suivantes. Identifiez chaque élément dynamique en entrant son nom, par exemple `sessionID` et sélectionnez Ajouter à en tant que valeur. L'option Ajouter à indique que l'élément doit être transmis aux étapes suivantes.

Remarque : Pour obtenir le nom d'un élément de page dynamique, affichez le code source HTML de la page sur laquelle il se trouve.

Les éléments de page dynamiques passent d'une transaction à la suivante. S'il n'est plus nécessaire qu'un élément de page soit transmis à une étape suivante, associez l'option Valeur de l'élément à Retirer de. Mettez à jour manuellement les étapes de transaction afin de garantir que les éléments de page corrects sont traités.

Utilisez les instructions suivantes pour ajouter et supprimer des éléments de page dynamiques :

- Si une étape n'utilise pas d'élément de page dynamique, ne sélectionnez pas DYNAMIC en tant que type de paramètre.
- Si une étape requiert un élément de page dynamique, l'étape qui extrait la page sur laquelle l'élément dynamique apparaît doit spécifier le nom de l'élément et la valeur Ajouter à.
- Si une étape ne requiert pas d'élément dynamique provenant d'étapes précédentes, sélectionnez Retirer de pour la valeur de l'étape précédente.

GET et POST

Dans les méthodes `GET`, tous les éléments de page dynamiques sont insérés automatiquement dans l'URL de demande. Dans les méthodes `POST`, vous devez indiquer chaque élément dynamique en tant que paramètre FORM dans l'onglet Paramètres.

Le moniteur insère automatiquement les valeurs dynamiques pour chaque formulaire lors de l'exécution de l'étape de transaction.

Création de transaction

Vous définissez des transactions en créant des éléments de profil et des étapes de transaction TRANSX à l'aide de l'interface utilisateur Internet Service Monitoring. Voir «Création de transactions», à la page 405

Configuration du test des services du moniteur TRANSX

Tableau 112. Configuration du moniteur TRANSX

Zone	Description
transxname	Nom de la transaction.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`

Remarque : Surveillez la disponibilité d'un site Web à l'aide d'une séquence de navigation Web, de téléchargement de fichier et d'envoi d'e-mails.

1. Créez un élément de profil TRANSX.
2. Créez une étape de transaction HTTP pour surveiller la disponibilité d'un site Web.
3. Créez une étape de transaction FTP pour surveiller un téléchargement de fichier.
4. Créez une étape de transaction POP3 ou SMTP pour surveiller les e-mails.

Pour plus d'informations, reportez-vous à la documentation de chaque moniteur.

Eléments du moniteur

Le moniteur TRANSX génère des événements contenant les résultats de chaque transaction. Ces événements contiennent les résultats de l'ensemble de la transaction, ainsi que ceux des différentes étapes de la transaction.

Par défaut, le moniteur place tous les résultats de transaction et d'étape dans un seul événement, mais en utilisant la propriété `MultipleEvents`, vous pouvez configurer le moniteur pour créer des événements spécifiques pour chaque étape de transaction et un événement récapitulatif pour l'ensemble de la transaction. Le tableau 1 répertorie les éléments récapitulatifs TRANSX.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 113. Eléments de moniteur récapitulatifs TRANSX

Elément	Description
$numberOfSteps*(NumberOfSteps)	Nombre d'étapes de la transaction.
$stepDescriptions	Liste des descriptions de chaque étape, séparées par un caractère de barre verticale (|).
$stepTimes*(Step*1 to 10*TotalTime)	Données de durée renvoyées par chaque étape (1 à 10).
$stepUnits	Liste des unités de chaque étape, généralement des secondes, séparées par un caractère de barre verticale (|).
(TransName)	Nom de la transaction, spécifié lors de la configuration de la transaction.
(TransStepDescription)	Description de l'étape de transaction, spécifiée lors de la configuration de l'étape.

Message d'état

Le moniteur TRANSX fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état.

Tableau 114. Messages d'état du moniteur TRANSX

Message	Description
Successfully completed transaction	La transaction a abouti.
Error in transaction	Un incident est survenu dans l'une des étapes de la transaction.
Service Level Failed, ending transactionService Level Failed	Le niveau de service de l'une des étapes a renvoyé une réponse d'échec, qui a provoqué l'arrêt de la transaction.

Création de transactions :

Les transactions peuvent être définies en créant des éléments de profil et des étapes de transaction TRANSX à l'aide de l'interface utilisateur Internet Service Monitoring.

Procédure

Pour créer une transaction à l'aide de l'interface, procédez comme suit :

1. Cliquez sur l'icône **Configuration système**. Cliquez ensuite sur **Configuration d'agent**. La fenêtre Configuration d'agent s'ouvre.
2. Cliquez sur l'onglet **ISM** pour configurer l'agent Internet Service Monitoring.
3. Cliquez sur l'icône plus **(+)** pour créer un nouveau profil. Entrez le **Nom de profil** et la **Description**.
4. Cliquez sur **Suivant**.
5. Cliquez sur Moniteur **TRANSX** dans la liste déroulante du moniteur pour sélectionner Moniteur TRANSX.
6. Cliquez sur **Suivant**.
7. Entrez les paramètres obligatoires.
8. Dans l'onglet **Avancé**, indiquez la **Fréquence de sondage**.

9. Cliquez sur l'icône plus **(+)** dans l'onglet Etapes.
10. Cliquez sur le moniteur qui doit être sélectionné dans la liste déroulante du moniteur.
11. Cliquez sur **Sélectionner** pour configurer l'étape de la transaction.
    a. Indiquez les paramètres obligatoires et facultatifs de la même manière que lorsqu'ils ont précédemment été entrés pour configurer les éléments de profil.
    b. Si vous créez des étapes dynamiques pour le moniteur HTTP ou HTTPS, définissez les paires Nom et Valeur dans l'onglet Paramètres, puis sélectionnez DYNAMIC comme type de paramètre.
12. Cliquez sur **Ajouter**.
13. Cliquez sur l'icône Actualiser dans la grille des étapes.
14. Répétez les étapes 1 à 13 pour chaque transaction supplémentaire.
15. Cliquez sur **Ajouter** pour terminer.
16. Cliquez sur **Terminé** pour sauvegarder.

Résultats

Remarque : Pour spécifier une pause entre chaque étape de la transaction, utilisez la propriété `StepPause`.

Paramètre SSL dans Internet Service Monitoring

Internet Service Monitoring utilise OpenSSL pour communiquer en toute sécurité avec des services Internet généralement distants à l'aide de différents moniteurs ; par exemple, le moniteur HTTPS communique avec un service HTTPD sécurisé. Internet Service Monitoring utilise également OpenSSL entre les moniteurs et Databridge et entre l'agent Internet Service Monitoring (KIS) et Databridge. Indiquez la suite de chiffrement que votre application utilise dans la propriété `SSLCipherSuite`.

Databridge doit être configuré pour communiquer de manière sécurisée avec les moniteurs et l'agent Internet Service Monitoring afin que chaque moniteur partage un ensemble commun de propriétés liées à Databridge pour gérer la communication sécurisée avec ce dernier. Certains moniteurs partagent également un ensemble comparable mais différent de propriétés connexes pour gérer les communications sécurisées avec leurs services Internet testés respectifs.

Les moniteurs suivants prennent en charge la surveillance de services Internet sécurisés :

- HTTPS
- IMAP4
- POP3
- SMTP

Ces moniteurs utilisent des certificats. Tous les certificats sont stockés au format X509 dans Privacy Enhanced Mail .Pemfiles dans `$ISMHOME/certificates`. Le certificat de Databridge est stocké au même endroit. C'est la raison pour laquelle les propriétés suivantes sont partagées par tous les moniteurs, Databridge et l'agent Internet Service Monitoring :

- SSLTrustStore (par défaut : $ISMHOME/certificates/trust.pem)
- SSLTrustStorePath (par défaut : $ISMHOME/certificates/)

Comme toutes les communications entre les moniteurs et Databridge et entre des moniteurs sélectionnés et leurs services Internet sécurisés s'appuient sur la même version d'OpenSSL, elles partagent un certain nombre de propriétés. Par exemple, le niveau maximal de sécurité qu'Internet Service Monitoring peut fournir est une fonction du plus haut niveau de sécurité fourni par le protocole OpenSSL sous-jacent. De la même manière, le niveau minimal de sécurité fourni est dépendant du protocole OpenSSL sous-jacent.

Si Internet Service Monitoring est mis à jour et que l'OpenSSL sous-jacent est concerné, les services Internet surveillés peuvent en être affectés. Par exemple :

1. Le moniteur HTTPS dans Internet Service Monitoring V7.x.1 surveille un serveur HTTPD sécurisé.

2. Appliquez une nouvelle version d'Internet Service Monitoring qui contient une version mise à jour d'OpenSSL, ce qui signifie que le moniteur HTTPS est maintenant au niveau de version V7.x.2.
3. Vous constatez que le moniteur HTTPS ne parvient plus à surveiller le processus HTTPD sécurisé.

Le niveau de sécurité du serveur HTTPD est inférieur au niveau minimal pris en charge par la nouvelle version d'Internet Service Monitoring V7.x.2. Si la configuration du moniteur HTTPS n'a pas changé, son comportement, lui, a changé car il dépend de la couche OpenSSL sous-jacente. La combinaison plus récente d'Internet Service Monitoring/moniteur HTTPS /OpenSSL est plus sécurisée que l'ancienne et il est nécessaire à présent d'élever le niveau de sécurité du serveur HTTPD distant.

La surveillance des services Internet sécurisés vous mettent face à un dilemme. Le niveau de sécurité d'Internet Service Monitoring doit-il être maintenu à un niveau faible pour permettre la surveillance des services Internet bénéficiant d'une protection réduite ou doit-il être relevé pour atteindre le niveau minimal requis par les paramètres recommandés actuels ? Dans la première hypothèse, Internet Service Monitoring est affaibli et la sécurité risque d'être compromise, peut-être même aux deux extrémités.

La même version d'OpenSSL est utilisée par tous les moniteurs. Tous ces moniteurs partagent un ensemble commun de propriétés décrites dans le tableau ci-après pour configurer la couche OpenSSL sous-jacente.

Tableau 115. Propriétés de moniteur liées à OpenSSL

Nom de la propriété	Paramètre de la propriété	Description
`SSLCipherSuite`	chaîne	Indique les suites de chiffrement à utiliser pour des opérations SSL entre le moniteur et le service Internet surveillé. Les valeurs de cette propriété doivent être indiquées dans un format recommandé par OpenSSL. Valeur par défaut : `AES:3DES:DES:!EXP:!DHE:!EDH`
`SSLDisableSSLv2`	`0` | `1`	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – SSLv2 est autorisé `1` – SSLv2 n'est PAS autorisé Valeur par défaut : 1 (SSLv2 n'est PAS autorisé).
`SSLDisableSSLv3`	`0` | `1`	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – SSLv3 est autorisé `1` – SSLv3 n'est PAS autorisé Valeur par défaut : 1 (SSLv3 n'est PAS autorisé).
`SSLDisableTLS`	`0` | `1`	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – TLSv1.0 est autorisé `1` – TLSv1.0 n'est PAS autorisé Valeur par défaut : `0` (TLSv1.0 est autorisé).
`SSLDisableTLS11`	`0` | `1`	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – TLSv1.1 est autorisé `1` – TLSv1.1 n'est PAS autorisé Valeur par défaut : 0 (TLSv1.1 est autorisé).

Tableau 115. Propriétés de moniteur liées à OpenSSL (suite)

Nom de la propriété	Paramètre de la propriété	Description
SSLDisableTLS12	0|1	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. 0 – TLSv1.2 est autorisé 1 – TLSv1.2 n'est PAS autorisé Valeur par défaut : 0 (TLSv1.2 est autorisé).
SSLCertificateFile	chaîne	Chemin et nom du fichier de certificat numérique public utilisé par le moniteur. Lorsqu'un moniteur tente d'établir une connexion à un service Internet, ce dernier peut exiger de lui qu'il fournisse un certificat côté client, pour lui permettre de vérifier le moniteur ou le client (vérification du certificat côté client). Le certificat doivent être au format PEM (Privacy Enhanced Mail). Pour le moniteur HTTPS, cette valeur peut être définie pour chaque élément HTTPS au moment de la création. Toutefois, si le moniteur HTTPS doit utiliser le même certificat pour tous les éléments, la valeur du fichier HTTPS.props est utilisée. Pour les moniteurs IMAP, LDAP, POP3, SIP, SMTP et SOAP, la valeur est définie au niveau du moniteur. Si le chemin d'accès n'est pas absolu, il est interprété par le moniteur comme étant relatif par rapport au répertoire de travail, $ISMHOME/certificates. Valeur par défaut : ""
SSLKeyFile	chaîne	Chemin et nom du fichier contenant la clé privée utilisée par le moniteur. Le moniteur utilise ce fichier pour chiffrer les messages qu'il l'envoie aux autres. Les récepteurs utilisent le certificat numérique public du moniteur pour déchiffrer le message. Valeur par défaut : monitoryKey.pem
SSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL. Valeur par défaut : ""

Tableau 115. Propriétés de moniteur liées à OpenSSL (suite)

Nom de la propriété	Paramètre de la propriété	Description
`SSLTrustStoreFile`	chaîne	Nom complet du fichier qui stocke tous les certificats publics X509 des services Internet surveillés sous la forme d'une liste concaténée. Les certificats révoqués (CRL) sont également stockés ici sous la forme d'une liste concaténée. Databridge peut également stocker son certificat public ici. Cette propriété apparaît dans le fichier `bridge.props`. Les certificats sont stockés au format PEM (Privacy Enhanced Mail). Convertissez au format PEM les certificats obtenus dans d'autres formats à l'aide des logiciels OpenSSL disponibles sur le site http://www.openssl.org. Valeur par défaut : **`"$ISMHOME/certificates/trust.pem"`**
`SSLTrustStorePath`	chaîne	Emplacement des fichiers `.pem` contenant les certificats X509 du service Internet sécurisé surveillé. Les certificats révoqués (CRL) sont également stockés ici. Databridge peut également stocker son certificat public ici. Cette propriété apparaît dans le fichier `bridge.props`. Si de nouveaux certificats sont ajoutés à ce répertoire, exécutez la commande openssl `rehash` pour analyser le répertoire et calculer un hachage pour chaque certificat. Si les propriétés `SSLTrustStoreFile` et `SSLTrustStorePath` sont toutes les deux utilisées, OpenSSL utilise les deux propriétés pour localiser les certificats de confiance. Valeur par défaut : `"$ISMHOME/certificates/"`
`VerifyCertificate Preference`	0|1	Active ou désactive la vérification du certificat fourni par le service Internet surveillé en fonction de la liste de révocation de certificat (CRL). Valeur par défaut : 0 - désactivé

Suites de chiffrement

Les suites de chiffrement dont disposent Internet Service Monitoring sont un sous-ensemble des suites autorisées par OpenSSL. L'ensemble de suites de chiffrement autorisées par OpenSSL change au fil du temps. Au fur et à mesure que de nouvelles vulnérabilités sont détectées et que les meilleures pratiques évoluent, l'accès à des types spécifiques et généraux de suites de chiffrement peut être limité ou supprimé intégralement par OpenSSL. Ces versions ultérieures d'OpenSSL étant incluses dans les versions ultérieures d'ISM, les effets produits peuvent avoir une incidence sur la configuration et le fonctionnement des moniteurs.

Utilisez la propriété SSLCipherSuite au niveau du moniteur pour indiquer les suites de chiffrement autorisés par un moniteur à partir de toutes les suites de chiffrement disponibles à l'aide de mots clés. Pour indiquer plusieurs suites, utilisez une liste de mots clés séparés par le signe deux points. Par exemple, la propriété SSLCipherSuite par défaut est `AES:3DES:DES:!EXP:!DHE:!EDH`. Cette sélection signifie que les suites de chiffrement incluant AES, 3DES et DES sont autorisées mais les suites de chiffrement qui utilisent les échanges de clés EXP

(Export short key lengths)), DHE (Diffie Hellman Exchange) ou EDH (Ephemeral Diffie Hellman) sont exclus. Lorsque la connexion sécurisée est établie entre le moniteur et le service Internet, AES est utilisé en premier, suivi de 3DES, puis de DES, si nécessaire. La syntaxe de la suite de chiffrement pour Internet Service Monitoring est la même que pour OpenSSL.

Pour sélectionner l'ensemble de suites de chiffrement approprié pour un moniteur, examinez les algorithmes pris en charge par la couche OpenSSL sous-jacente, la plage de suites de chiffrement prises en charge par le service Internet surveillé et les normes de sécurité de votre organisation. Vous ne pourrez peut-être pas surveiller un site externe sécurisé dont le niveau de sécurité est inférieur à celui que Internet Service Monitoring ou OpenSSL tolère. Dans certains cas, un moniteur qui pouvait auparavant surveiller un service Internet risque d'échouer après avoir mis à niveau Internet Service Monitoring car les niveaux de sécurité sont incompatibles.

Le tableau ci-dessous répertorie un sous-ensemble de suites de chiffrement équivalent à la propriété SSLCiperSuite par défaut incluant `AES:3DES:DES:!EXP:!DHE:!EDH` avec leurs propriétés. Les termes suivants apparaîtront dans le tableau :

- Nom de la suite de chiffrement : décrit la suite de chiffrement à l'aide d'un nom construit à partir de mots clés.
- Protocole : décrit la version du protocole pris en charge.
- Echange de clés : décrit le système d'échange de clés utilisé pour le chiffrement et le déchiffrement.
- Chiffrement et longueur de la clé : décrit le type d'algorithme de chiffrement utilisé et la longueur de la clé (en bits) utilisée.
- MAC : décrit le code d'authentification de message (Message Authentication Code) utilisé pour s'assurer que les données n'ont pas été faussées.

Tableau 116. Nom de la suite de chiffrement et valeurs de propriété `AES:3DES:DES:!EXP:!DHE:!EDH`

Nom de la suite de chiffrement	Protocole	Echange de clés	Authentification	Chiffrement et longueur de clé	Code d'authentification de message
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	SRP	DSS	AES(256)	SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	SRP	RSA	AES(256)	SHA1
SRP-AES-256-CBC-SHA	SSLv3	SRP	SRP	AES(256)	SHA1
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM(256)	AEAD
...suivi de 61 lignes supplémentaires					

Le tableau ci-dessous répertorie un sous-ensemble de suites de chiffrement équivalent à la valeur de la propriété `SSLCiperSuite` incluant `AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3` avec leur propriétés. Certains protocoles sont maintenant élimités et l'ensemble global des suites de chiffrement est réduit de 71 à 31.

Tableau 117. Nom de la suite de chiffrement et valeurs de propriétés **`AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3`**

Nom de la suite de chiffrement	Protocole	Echange de clés	Authentification	Chiffrement et longueur de clé	Code d'authentification de message
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM(256)	AEAD
DH-RSA-AES256-GCM-SHA384	TLSv1.2	DH/RSA	DH	AESGCM(256)	AEAD
DH-RSA-AES256-SHA256	TLSv1.2	DH/RSA	DH	AES(256)	SHA256
DH-DSS-AES256-SHA256	TLSv1.2	DH/DSS	DH	AES(256)	SHA256
ADH-AES256-GCM-SHA384	TLSv1.2	DH	Aucun	AESGCM(256)	AEAD
ADH-AES256-SHA256	TLSv1.2	DH	Aucun	AES(256)	SHA256
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH/RSA	ECDH	AESGCM(256)	AEAD
...suivi de 21 lignes supplémentaires					

Réduction des vulnérabilités

Les chiffrements DHE et EDH seront désactivés par défaut dans les éditions ultérieures en raison de vulnérabilités. Pour les versions antérieures d'Internet Service Monitoring, il peut s'avérer nécessaire de désactiver les chiffrements DHE et EDH dans tous les moniteurs. Pour désactiver les chiffrements DHE et EDH, mettez à jour les propriétés `SSLCipherSuite` et `BridgeSSLCipherSet` des moniteurs.

Par exemple, pour désactiver des chiffrements DHE et EDH dans le moniteur HTTPS, mettez à jour le fichier `https.props` pour inclure les propriétés suivantes :

```
SSLCipherSuite: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!EDH
BridgeSSLCipherSet: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!ED
```

Assurez-vous que cette modification de configuration n'entraîne pas de problèmes de compatibilité. Si vous modifiez le paramètre par défaut après l'application de ce correctif, vous risquez de vous exposer à une vulnérabilité en matière de sécurité. Vous devez examiner l'ensemble de votre environnement pour identifier les autres emplacements où vous avez activé le protocole d'échange de clés Diffie-Hellman utilisé dans TLS et exécutez les actions d'atténuation et de correction appropriées.

Sélection de protocoles

Vous pouvez faire votre choix parmi une série de protocoles de communication sécurisée anciens ou plus récents. Vous pouvez les sélectionner individuellement à l'aide d'un ensemble de propriétés de moniteur de type booléen :

- SSLDisableSSLv2
- SSLDisableSSLv3

- SSLDisableTLS
- SSLDisableTLS11
- SSLDisableTLS12
- BridgeSSLDisableSSLv2
- BridgeSSLDisableSSLv3

Vous devez désactiver SSLv2 et SSLv3. La sécurité de ces protocoles est compromise et présente plusieurs vulnérabilités connues. Ils sont désactivés par défaut et sont fournis uniquement pour des raisons .

Internet Service Monitoring active TLS par défaut. Si vous savez que les services Internet que vous surveillez n'utilisent pas TLS 1.0 et sont déjà passés à TLS 1.1 ou TLS 1.2, désactivez les protocoles inutilisés dans Internet Service Monitoring.

Le composant Databridge communique avec l'agent Internet Service Monitoring et chacun des moniteurs. Par défaut, cette communication est chiffrée et TLS est le protocole préféré.

Magasins de clés de confiance et certificats

Internet Service Monitoring stocke ses certificats dans un fichier et dans un emplacement définis par l'utilisateur. Tous les certificats doivent être stockés au format PEM (Privacy Enhanced Mail). Vérifiez que les certificats publics obtenus auprès d'autres organisations sont convertis au format PEM. Des logiciels de conversion sont disponibles à l'adresse http://www.openssl.org.

Les certificats de confiance indiqués à l'aide de la propriété `SSLTrustStoreFile` sont stockés dans le fichier sous la forme d'une liste concaténée.

Il est recommandé de stocker les listes de révocation de certificats (CRL) dans le magasin de clés de confiance dans lequel les certificats peuvent être validés. Les autorités de certification ont mis en place des systèmes qui génèrent des listes de certificats révoqués, ainsi que des systèmes de distribution qui les rendent disponibles publiquement. Ainsi, tout certificat compromis est révoqué.

Paramètres de sécurité de Databridge

Tous les moniteurs communiquent avec Databridge ; ils possèdent donc tous un ensemble commun de propriétés qui doivent être définies pour gérer les communications entre les moniteurs et Databridge. Par défaut, la communication est chiffrée. Le protocole de chiffrement par défaut est TLS. Contrairement aux propriétés des moniteurs, il n'y a pas de mécanisme pour contrôler si une version spécifique de TLS est activée ou désactivée. Tous les moniteurs doivent posséder les mêmes valeurs pour les propriétés Databridge. Sinon, des problèmes de communication apparaissent. De la même manière, les propriétés définies dans le fichier .props de Databridge doivent être cohérentes avec celles des moniteurs. Databridge communique également avec l'agent Internet Service Monitoring qui possède son propre fichier .props. Certaines des valeurs du fichier .props sont liées à Databridge et comme pour les moniteurs, elles doivent posséder des valeurs cohérentes avec celles définies dans le fichier `.props` de Databridge.

Tableau 118. Propriétés de Databridge liées à OpenSSL

Nom de la propriété	Paramètre de la propriété	Description
`BridgeSSLEncryption`	`0`|`1`	Détermine si les communications avec Databridge sont chiffrées ou non. Cette propriété couvre toutes les communications de Databridge vers les moniteurs et l'agent Internet Service Monitoring. `0` – non chiffré `1` – chiffré **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge.

Tableau 118. Propriétés de Databridge liées à OpenSSL (suite)

Nom de la propriété	Paramètre de la propriété	Description
BridgeSSLCipherSet	chaîne	Indique les suites de chiffrement à utiliser pour des opérations SSL en provenance et à destination de Databridge. Les valeurs de cette propriété doivent être indiquées dans le format recommandé par OpenSSL. **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : `AES:3DES:DES:!EXP:!DHE:!EDH`
BridgeSSLDisableSSLv2	0 | 1	Détermine le type de connexion sécurisée à créer en provenance et à destination de Databridge. `0` – SSLv2 et SSLv3 sont autorisés `1` – SSLv2 n'est PAS autorisé **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : 1 (SSLv2 n'est PAS autorisé).
BridgeSSLDisableSSLv3	0 | 1	Détermine le type de connexion sécurisée à créer en provenance et à destination de Databridge. `0` – SSLv3 est autorisé `1` – SSLv3 n'est PAS autorisé **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : 1 (SSLv3 n'est PAS autorisé).
BridgeSSLCertificateFile	chaîne	Chemin et nom de fichier du certificat SSL Databridge numérique. Valeur par défaut : `$ISMHOME/certificates/bridgeCert.pem`
BridgeSSLKeyFile	chaîne	Chemin et nom du fichier de clé privée SSL Databridge. Valeur par défaut : `$ISMHOME/certificates/bridgeKey.pem`
BridgeSSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL Databridge. Valeur par défaut : **Tivoli**

Tableau 118. Propriétés de Databridge liées à OpenSSL (suite)

Nom de la propriété	Paramètre de la propriété	Description
BridgeSSLTrustStore	chaîne	Chemin et nom du fichier de certificat sécurisé pour l'authentification. Cette propriété est nécessaire uniquement lorsque vous utilisez la propriété **BridgeSSLAuthenticatePeer**. Valeur par défaut : `$ISMHOME/certificates/trust.pem` Si vous souhaitez configurer l'authentification SSL entre un moniteur et Databridge, ou entre Databridge et l'agent, associez `BridgeSSLAuthenticatePeer` à la valeur 1 et redémarrez Databridge. Cette action permet d'authentifier les certificats du serveur. Vous pouvez stocker des certificats à la fois dans `SSLTrustStoreFile` et `SSLTrustStorePath`. Valeurs par défaut : • `SSLTrustStoreFile`, `$ISMHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISMHOME/certificates/` Pour ajouter de nouveaux certificats, effectuez l'une des étapes suivantes : • Ajoutez un certificat à la fin de la liste dans le fichier texte `SSLTrustStoreFile` • Ajoutez un nouveau certificat au répertoire `SSLTrustStorePath`, et exécutez la commande OpenSSL **c_rehash certificate_dir** pour hacher les certificats
SSLTrustStoreFile	chaîne	Cette propriété est utilisée par des moniteurs sécurisés et Databridge. Pour plus d'informations, voir tableau 115 , à la page 407.
SSLTrustStorePath	chaîne	Cette propriété est utilisée par des moniteurs sécurisés et Databridge. Pour plus d'informations, voir tableau 115 , à la page 407.
BridgeSSLAuthenticatePeer	0 | 1	Indique si Databridge doit effectuer une authentification croisée avec d'autres composants Internet Service Monitoring. `0` – désactivé `1` – activé Si un moniteur entre en contact avec Databridge, il doit s'authentifier auprès de Databridge et Databridge doit s'authentifier auprès du moniteur. Si l'agent Internet Service Monitoring contacte Databridge, il doit s'authentifier auprès de Databridge et Databridge doit s'authentifier auprès de l'agent. Les certificats de Databridge sont stockés dans BridgeSSLTrustStore. Valeur par défaut : 0 - désactivé

Propriétés de l'agent Internet Service Monitoring

L'agent Internet Service Monitoring possède son propre fichier de propriétés qui contient un ensemble de propriétés et de paramètres de sécurité. Le fichier de propriétés de l'agent ne communique pas avec les moniteurs, mais il communique avec Databridge, de sorte que les paramètres de sécurité définis dans le fichier `.props` de l'agent gèrent la communication entre l'agent et Databridge.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes Windows à l'aide de la fenêtre IBM Performance Management.

Procédure

Configurez l'agent Internet Service Monitoring sur le système utilisateur de la manière suivante. Pour configurer manuellement l'agent Internet Service Monitoring sur les systèmes utilisateur :

1. Dans le tableau de bord IBM Performance Management, cliquez sur **Configuration système** > **Configuration d'agent** sous **Configuration système**.
2. Cliquez sur l'onglet **ISM** pour ouvrir le tableau de bord de l'agent Internet Service Monitoring.

Configuration de Databridge

La configuration de Databridge comprend la définition de propriétés qui en contrôlent le fonctionnement, comme la connexion des modules du composant et des moniteurs de service Internet.

Fonctionnement et configuration :

Databridge et ses modules de composant sont configurés à l'aide de fichiers de propriétés.

Les propriétés déterminent le fonctionnement de Databridge et de ses modules de composant qui envoient les résultats de test à IBM Cloud Application Performance Management en vue de la génération de rapport dans le tableau de bord de l'agent Internet Service Monitoring.

Configuration de Databridge :

Databridge doit être configuré de sorte à recevoir des données provenant des moniteurs de service Internet et les transmettre à ses modules pour un traitement plus poussé.

Le tableau suivant répertorie les fichiers associés à Databridge. Le **fichier de propriétés**, le **fichier SAF (Store And Forward)** et le **fichier journal** sont décrits en détail dans leurs sections respectives.

Tableau 119. Fichiers Databridge et leur emplacement

Fichier Databridge	Emplacement ou nom
Fichier exécutable	`$ISHOME/platform/arch/bin/nco_m_bridge`
Fichier de propriétés	`$ISHOME/etc/props/bridge.props`
Fichier SAF (Store and Forward) and Forward) and Forward	Le nom et l'emplacement sont définis par les propriétés dans le fichier `bridge.props`. Le nom et l'emplacement par défaut sont `$ISHOME/var/sm_bridge.saf`
Fichier journal	`$ISHOME/log/bridge.log`
Fichier journal des erreurs	`$ISHOME/log/bridge.err`

Fichier SAF (Store And Forward) :

Si Databridge ne peut pas transmettre des données à Netcool/OMNIbus, il stocke toutes les données qu'il doit normalement envoyer dans un fichier SAF (Store And Forward). Lorsque Netcool/OMNIbus est à nouveau disponible, il traite tous les événements stockés dans le fichier SAF.

Les propriétés QFile et QSize du fichier de propriétés Databridge déterminent le nom, l'emplacement et le fonctionnement du traitement SAF (Store and Forward).

Fichier journal
Databridge envoie des messages quotidiens concernant ses opérations à un fichier journal des messages. Par défaut, le nom de ce fichier est `$ISHOME/log/bridge.log`. Il est mis à jour à minuit (12:00 am). Les propriétés MsgDailyLog et MsgTimeLog de Databridge contrôlent l'opération de journalisation des messages.

Démarrage de Databridge :

Démarrage de Databridge à l'aide de la console Windows Services.

Procédure

Remarque : Si le module ObjectServer est connecté à Databridge, vérifiez que son système cible est en cours d'exécution avant de démarrer Databridge. Si les modules Databridge ne parviennent pas à s'initialiser correctement, Databridge ne démarre pas.

1. A partir du bureau Windows, cliquez sur **Démarrer** > **Outils d'administration** > **Services**.
2. Dans la liste des services, sélectionnez le service NCO BRIDGE Internet Service Monitor et cliquez sur **Démarrer** dans le menu.

Connexion des modules :

Le fichier de propriétés Databridge définit les modules à connecter à Databridge.

Pourquoi et quand exécuter cette tâche

Chaque paire de propriétés Module n `SharedLib` et Module n `PropFile` définit la connexion d'un module. Les modules sont chargés dans l'ordre de définition en commençant par Module0.

Procédure

1. Pour connecter des modules spécifiques à Databridge, procédez comme suit :
   a. Dans le fichier de propriétés de Databridge, identifiez la paire de propriétés Module n `SharedLib` et Module n `PropFile` disponible suivante.
   b. Affectez à Module n `SharedLib` le nom de la bibliothèque partagée du module (son implémentation binaire).
   c. Affectez à Module n `PropFile` le chemin d'accès complet au fichier de propriétés du module.

   Dans cet exemple, les lignes 1 et 2 connectent le module ObjectServer, les lignes 3 et 4 connectent le module Datalog et les lignes 5 et 6 connectent le module IBM Application Performance Management (`pipe`). Le module Datalog n'a pas de fichier de propriétés. L'entrée du fichier de propriétés a donc pour valeur `""`.
2. Pour désactiver un module, procédez comme suit :
   a. Affectez la valeur `"NONE"` à la propriété Module n `SharedLib` correspondante, et la valeur `""` à la propriété Module n `PropFile`. Tous les autres modules d'une valeur supérieure à n sont également ignorés.

Connexion des moniteurs :

Les moniteurs de service Internet se connectent à Databridge via TCP. Chaque moniteur comporte un ensemble de propriétés qui configure la connexion à Databridge.

Pourquoi et quand exécuter cette tâche

Pour connecter un moniteur à Databridge, affectez la valeur de la propriété `SocketPort` définie dans le fichier de propriétés de Databridge à la propriété `BridgePort` définie dans le fichier de propriétés du moniteur. La valeur par défaut de chaque propriété `BridgePort` du moniteur et de la propriété `SocketPort` de Databridge est `9510`.

DataBridge prend en charge le chiffrement SSL des résultats de test envoyés par les moniteurs. Pour chiffrer les résultats de test du moniteur, affectez les valeurs des propriétés `BridgeSSL` définies dans le fichier de propriétés de Databridge aux propriétés `BridgeSSL` définies dans le fichier de propriétés Databridge. Pour chiffrer tous les résultats de test des moniteurs, tous les moniteurs doivent avoir les mêmes propriétés `BridgeSSL`.

Configuration du module Databridge :

Databridge transmet les résultats du test à l'agent Internet Service Monitoring. L'agent de surveillance convertit ces données dans le format approprié et les transmet au serveur IBM Application Performance Management. Configurez le module Databridge et l'agent Internet Service Monitoring via leurs fichiers de propriétés respectifs.

Configurez le fonctionnement de Databridge en modifiant les valeurs de propriétés définies dans le fichier de propriétés du module.

Le fichier de propriétés du module s'appelle `pipe_module.props`. Ce fichier se trouve dans le répertoire `$ISHOME/etc/props/`.

Le tableau ci-après répertorie les propriétés disponibles pour le module. Si vous apportez des modifications aux propriétés, vous devez redémarrer Databridge pour que ces modifications s'appliquent.

Tableau 120. Propriétés du module Databridge

Nom de la propriété	Type	Description
`TEMAHOST`	chaîne	Nom du système hôte qui exécute l'agent de surveillance. Valeur par défaut : `localhost`
`TEMAPORT`	entier	Numéro de port utilisé par l'hôte. Valeur par défaut : `9520`

Vous pouvez configurer le fonctionnement de l'agent Internet Service Monitoring en modifiant les valeurs de propriétés définies dans le fichier de propriétés de l'agent.

Le fichier de propriétés de l'agent de surveillance s'appelle `kisagent.props`. Il se trouve dans le répertoire `$ISMHOME/etc/props/`.

Le tableau suivant répertorie les propriétés disponibles pour l'agent de surveillance.

Tableau 121. Propriétés de l'agent de surveillance

Nom de la propriété	Type	Description
`TEMAPORT`	entier	Numéro de port utilisé par l'hôte. Il doit correspondre au numéro de port de la propriété `TEMAPORT` indiquée dans le fichier de propriétés du module. Valeur par défaut : `9520`

Tableau 121. Propriétés de l'agent de surveillance (suite)

Nom de la propriété	Type	Description
`ObsoleteDuration`	entier	Délai, en secondes, à l'issue duquel les données qui n'ont pas été mises à jour sont supprimées de la mémoire de l'agent de surveillance. Les données ne peuvent pas être mises à jour si, par exemple, un élément de profil a été arrêté ou qu'une défaillance du réseau s'est produite. **Remarque :** N'affectez pas à la propriété `ObsoleteDuration` une valeur inférieure à l'intervalle d'interrogation car cela risque d'entraîner des pertes de données entre les intervalles d'interrogation. Valeur par défaut : `900`
`AggDuration`	entier	Période, en secondes, à l'issue de laquelle l'agent de surveillance arrête l'agrégation et l'affichage des données dans le tableau de bord de l'agent. Toutes les données antérieures à l'heure indiquée sont supprimées de la mémoire de l'agent de surveillance. Les données antérieures sont calculées en comparant l'intervalle entre l'heure de début et l'heure actuelle à l'heure de la durée d'agrégation. Si l'intervalle est supérieur à la durée d'agrégation, 10 % des anciennes données sont supprimées et l'heure de début est augmentée d'un dixième de l'intervalle. L'agent de surveillance exécute ce calcul toutes les 5 minutes. Valeur par défaut : `3600`
`ManageServices`	`0|1`	Démarre et arrête tous les moniteurs et Databridge lorsque l'agent Internet Service Monitoring est démarré ou arrêté. `1` correspond à Activé et `0` correspond à Désactivé. Valeur par défaut : `1`

La connexion entre l'agent Internet Service Monitoring et le module Databridge est créée lorsque vous installez Internet Service Monitoring.

Configuration de la surveillance de J2SE

Pour collecter les données de surveillance et de diagnostic des ressources des applications Java sur site surveillées, vous devez configurer le collecteur de données J2SE.

Avant de commencer

Installez l'un des environnements d'exécution Java pris en charge :

- Oracle Java Platform Standard Edition 7 (kit de développement Java SE 7)

  A faire : Cet environnement Java Runtime ne prend pas en charge l'image du collecteur de données J2SE qui est configurée avec le protocole HTTPS.
- Oracle Java Platform Standard Edition 7 (Java SE Runtime Environment 7)

  A faire : Cet environnement Java Runtime ne prend pas en charge l'image du collecteur de données J2SE qui est configurée avec le protocole HTTPS.
- Oracle Java Platform Standard Edition 8 (kit de développement Java SE 8)
- Oracle Java Platform Standard Edition 8 (Java SE Runtime Environment 8)

- IBM SDK, Java Technology Edition, version 7
- IBM SDK, Java Technology Edition, version 8

Important : Pour Windows Server 2016, installez le kit de développement Java SE 8, mise à jour 131 (JDK 8u131) ou Java SE Development Kit 7, mise à jour 80 (JDK 7u80).

Pour plus d'informations sur la configuration système requise, voir Software Product Compatibility Reports for J2SE data collector.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le collecteur de données J2SE sur les systèmes Windows, Linux et AIX.

Procédure

1. Copiez les fichiers suivants du programme d'installation d'APM dans un répertoire :

   Important : le chemin de répertoire ne doit pas contenir d'espace.
   - Windows Copiez le fichier `gdc.zip` du programme d'installation d'APM dans un répertoire et extrayez-le.
   - Linux AIX Copiez le fichier `gdc-apd.tar.gz` du programme d'installation d'APM dans un répertoire et extrayez-le.
   - Linux AIX Accordez à l'utilisateur des droits en lecture/écriture et exécution sur le dossier `j2se_dc`. Les droits en exécution sont fournis pour l'exécution des scripts et des fichiers `JAR` dans le dossier. Les droits en lecture/écriture sont fournis car les fichiers de diagnostic approfondi sont générés dans ce dossier.
2. Sur la ligne de commande, accédez à *DCHOME*`\.gdc\<version_kit_outils>\bin` Où *version_kit_outils* correspond à :
   - Pour la version 8.1.4.0 et antérieure, *version_kit_outils* est 7.3.0.5.0.
   - Pour la version 8.1.4.0.1 et ultérieure, *version_kit_outils* est 7.3.0.14.0.
3. Exécutez la commande suivante :

   Windows `config.bat`

   Linux AIX `config.sh`
4. Lorsque vous y êtes invité, indiquez le chemin d'accès au répertoire de base Java et appuyez sur la touche Entrée. Par exemple,

   Windows `C:\Program Files\jre7`

   Linux AIX `/opt/ibm/java`
5. Procédez comme suit en vous référant à la version que vous utilisez.
   - Pour la version 8.1.4.0.2 et antérieure, procédez comme suit.
     a. Lorsque vous y êtes invité, entrez le nom complet (nom qualifié) de la classe principale de l'application et appuyez sur la touche Entrée. La classe principale est le point d'entrée de l'application qui doit être surveillée. Exemple : `testapp.TemperatureConveter`
     b. Lorsque vous y êtes invité, entrez un nom d'alias d'application distinct et appuyez sur la touche Entrée. Le nom indiqué est utilisé pour créer le nom d'instance sur le tableau de bord APM.

        Windows Le fichier `dcstartup.bat` est généré à l'emplacement suivant : *DCHOME*`\.gdc\`*version_kit_outils*`\runtime\j2se`*alias_application.nom_hôte.alias_application*. Ce fichier est le script permettant d'exécuter votre application avec le collecteur de données.

        Linux AIX Le fichier `dcstartup.sh` est généré à l'emplacement suivant : *DCHOME*`/.gdc/`*version_kit_outils*`/runtime/j2se`*alias_application.nom_hôte.alias_application*. Ce fichier est le script permettant d'exécuter votre application avec le collecteur de données.

- Pour la version 8.1.4.0.3 et ultérieure, procédez comme suit.
  a. A l'invite, entrez le répertoire de base de l'application Java. Par exemple, `/root/J2seApp/`
  b. Sélectionnez l'application Java dans la liste qui s'affiche.

     `1)com.ibm.SampleApplication`

     `2)com.ibm.DBApplication`

     `3)com.ibm.SpringBootApplication`

     Sélectionnez une application à configurer répertoriée dans la liste ou saisissez 0 pour fournir une autre application non répertoriée.

     1) Si vous saisissez 0, entrez le `nom complet` de la classe Main de n'importe quelle autre application. Par exemple, `com.ibm.testApp.Main`
     2) Si une autre option est sélectionnée dans la liste, le nom d'alias est créé à partir du nom de la classe. Si le nom d'alias dépasse le nombre limite de caractères, réduisez ce nombre.

        Important : Le nombre limite de caractères pour le nom d'alias est calculé de sorte que `nom_alias + nom_hôte` ne dépasse pas 24 caractères.
  c. Si vous sélectionnez une option dans la liste fournie à l'étape précédente, copiez le script de démarrage `<DCHOME>/j2se_dc/.gdc/`*`version_kit_outils`*`/runtime/j2se<alias_application>.<nom_hôte>.<alias_application>` à l'emplacement de votre choix.

Pour la version 8.1.4.0.2 et antérieures, suivez l'étape 6 pour modifier le fichier Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`.

6. Pour modifier le fichier Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`, procédez comme suit :
   - Si les classes et les fichiers JAR de l'application sont fournis dans un seul fichier JAR, procédez comme suit :
     a. Ouvrez le fichier suivant :
        - Windows `dcstartup.bat`
        - Linux AIX `dcstartup.sh`
     b. Remplacez `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`nom complet de la classe principale`* par `$ITCAM_JVM_OPTS -jar` *`fichier jar de l'application`* et sauvegardez le fichier.
   - Si l'application utilise plusieurs fichiers JAR, procédez comme suit :
     a. Ouvrez le fichier suivant :
        - Windows `dcstartup.bat`
        - Linux AIX `dcstartup.sh`
     b. Définissez la variable *CLASSPATH* sur les fichiers JAR.
     c. Remplacez `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`nom complet de la classe principale`* par `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS -jar` *`fichier jar de l'application`* et sauvegardez le fichier.

        Le fichier JAR de l'application doit contenir la classe de l'application de messagerie.

Pour la version 8.1.4.0.3 et ultérieures, suivez l'étape 7 pour modifier le fichier Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`.

7. Procédez comme suit si l'application utilise plusieurs fichiers JAR.
   a. Ouvrez le fichier suivant :
      - Windows `dcstartup.bat`
      - Linux AIX `dcstartup.sh`
   b. Définissez la variable *CLASSPATH* sur les fichiers JAR.

8. Pour activer le diagnostic approfondi, modifiez le fichier `custom_request.xml` dans le chemin suivant et ajoutez des classes et des méthodes propres à l'application.

   Windows *DCHOME*\.gdc*version_kit_outils*\runtime\
   j2se*alias_application.nom_hôte.alias_application*\custom

   Linux AIX *DCHOME*/.gdc/*version_kit_outils*/runtime/
   j2se*alias_application.nom_hôte.alias_application*/custom

   Par exemple :

```
<edgeRequest>

<requestName>truncateDb</requestName>

<Matches>testApp.JDBC.DBManager</Matches>

<type>application</type>

<methodName>truncateDb</methodName>

</edgeRequest>
```

9. Exécutez la commande suivante :

   Windows `dcstartup.bat`

   Linux AIX `dcstartup.sh`

   L'application J2SE est démarrée avec le collecteur de données configuré.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par le collecteur de données dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Vérification du statut du suivi des transactions et de la collecte des données de diagnostic

Pour la version 8.1.0.3 et ultérieure, sur la page de configuration de l'agent, vous pouvez vérifier le statut du suivi des transactions et des données de diagnostic.

Pourquoi et quand exécuter cette tâche

Vous pouvez vérifier le statut du suivi des transactions et de la collecte des données de diagnostic à l'aide de deux commandes. Reportez-vous à la procédure pour en savoir plus sur les commandes associées.

Procédure

1. Utilisez la commande **config status**.
   a. Ouvrez le répertoire bin. Exécutez la commande suivante :

      Linux AIX **cd <DCHOME>/j2se_dc/.gdc/version_kit_outils/bin/**

      Windows **cd <DCHOME>\j2se_dc\.gdc\version_kit_outils\bin**

      Où *version_kit_outils* correspond à :
      - Pour la version 8.1.4.0 et antérieure, *version_kit_outils* est 7.3.0.5.0.
      - Pour la version 8.1.4.0.1 et ultérieure, *version_kit_outils* est 7.3.0.14.0.

   b. Entrez la commande suivante pour vérifier le statut :

Linux AIX **config.sh status**

Windows **config.bat status**

c. Sélectionnez dans la liste les applications Java portant un nom d'alias qui sont identifiées pour vérifier leur statut, ou quittez.
   1) ddperf
   2) Main
   3) Exit

2. Utilisez la commande **config status <nom_alias_application>**.
   a. Entrez la commande suivante pour ouvrir un répertoire :

      Linux AIX **cd <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/bin/**

      Windows **cd <DCHOME>\j2se_dc\.gdc\7.3.0.14.0\bin**

   b. Entrez la commande suivante pour vérifier le statut :

      Linux AIX **config.sh status <nom_alias_application>**

      Windows **config.bat status <nom_alias_application>**

Changement du statut du suivi des transactions et de la collecte des données de diagnostic

Pour la version 8.1.0.3 et ultérieure, sur la page de configuration de l'agent, vous pouvez changer le statut du suivi des transactions et des données de diagnostic.

Pourquoi et quand exécuter cette tâche

Vous pouvez changer le statut du suivi des transactions et de la collecte des données de diagnostic à l'aide de l'invite de commande. Reportez-vous à la procédure pour en savoir plus sur les commandes associées.

Procédure

1. Ouvrez le répertoire bin. Exécutez la commande suivante :

   Linux AIX **cd <DCHOME>/j2se_dc/.gdc/version_kit_outils/bin/**

   Windows **cd <DCHOME>\j2se_dc\.gdc\version_kit_outils\bin**

   Où *version_kit_outils* correspond à :
   - Pour la version 8.1.4.0 et antérieure, *version_kit_outils* est 7.3.0.5.0.
   - Pour la version 8.1.4.0.1 et ultérieure, *version_kit_outils* est 7.3.0.14.0.

2. Entrez la commande suivante pour vérifier le statut :

   Linux AIX **config.sh <nom_alias_application>**

   Windows **config.bat <nom_alias_application>**

3. A l'invite, sélectionnez l'option permettant d'activer ou de désactiver le suivi des transactions. La valeur par défaut est `Yes`.
4. A l'invite, sélectionnez l'option permettant d'activer ou de désactiver la collecte des données de diagnostic. La valeur par défaut est `Yes`.
   a. Si vous définissez la valeur Yes, sélectionnez l'option permettant d'activer ou de désactiver la trace de méthode. La valeur par défaut est `NO`.

Configuration de la surveillance de JBoss

L'Monitoring Agent for JBoss surveille les ressources des serveurs d'applications JBoss et de la plateforme JBoss Enterprise Application. Utilisez les tableaux de bord fournis avec l'agent JBoss pour identifier les applications et les demandes les plus lentes, les goulots d'étranglement dans le pool d'unités d'exécution, les problèmes de segment de mémoire JVM et de récupération de place, les sessions les plus actives et les autres goulots d'étranglement sur le serveur d'applications JBoss.

Avant de commencer

- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 122.

Tableau 122. Versions d'agent

Version d'agent	Documentation
1.0.3.3	Cloud APM 8.1.4
1.0.3.1	IBM Performance Management 8.1.3 [1]
1.0.2.11	IBM Performance Management 8.1.2 [1]

[1] Le lien ouvre une rubrique IBM Knowledge Center sur site.

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent JBoss. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent JBoss.
- Avant de configurer l'agent JBoss, le serveur JBoss doit d'abord être configuré en procédant comme suit :
  1. «Activer les connexions au serveur JMX MBean», à la page 425.
  2. «Ajout d'un utilisateur de gestion de serveur JBoss», à la page 426.
  3. «Activation de la collecte des statistiques Web/HTTP», à la page 427. Cette procédure est applicable à JBoss EAP version 7.x et WildFly versions 8.x, 9.x et 10.x.

Pourquoi et quand exécuter cette tâche

Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères.

Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous spécifiez `JBoss` comme nom d'instance, votre nom de système géré est `JBoss:hostname:JE`.

Remarque : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.

L'agent JBoss est un agent multi-instance. Vous devez créer une instance d'agent pour chaque serveur JBoss que vous surveillez et démarrer chaque instance d'agent manuellement.

La fonction de suivi des transactions est disponible pour l'agent JBoss dans l'offre Cloud APM, Advanced.

- Pour activer le suivi des transactions pour une nouvelle instance d'agent, suivez l'étape 1 ou l'étape 2 de cette procédure, puis suivez la procédure de «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 434.
- Pour activer le suivi des transactions pour une instance d'agent déjà configurée pour la surveillance de base, suivez la procédure de «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 434.

- Pour désactiver le suivi des transactions pour une instance d'agent, suivez la procédure de «Désactivation du collecteur de données du suivi des transactions de l'agent JBoss», à la page 437.
- Pour désinstaller le suivi des transactions pour toutes les instances d'agent et supprimer le kit d'outils de suivi des transactions, suivez la procédure de «Désinstallation du suivi des transactions de tous les agents JBoss», à la page 438.

Procédure

1. Configurez l'agent sur des systèmes Windows à l'aide de la fenêtre IBM Performance Management ou du fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 428.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 432.
2. Configurez l'agent sur des systèmes Linux en exécutant le script de ligne de commande et en répondant aux invites, ou à l'aide du fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 431.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 432.
3. Facultatif : Configurez le suivi des transactions en configurant des instances d'agent individuelles pour fournir les données de suivi des transactions et en configurant votre Tableau de bord d'Application Performance pour afficher les données de suivi des transactions.
   a. Suivez la procédure de «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 434.
   b. Activez les données de suivi des transactions dans le Tableau de bord d'Application Performance pour l'agent JBoss.
      1) Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
      2) Sélectionnez l'onglet **JBoss**.
      3) Sélectionnez les cases à cocher pour les instances de l'agent du serveur JBoss que vous souhaitez surveiller et effectuez l'une des actions suivantes figurant dans la liste **Actions** :
         - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Enabled*.
         - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Disabled*.
   c. Consultez les tableaux de bord des données de suivi des transaction de l'agent JBoss en ajoutant l'instance d'agent JBoss à une application dans votre Tableau de bord d'Application Performance. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.
   d. Assurez-vous que des comptes utilisateur sont affectés à un rôle qui inclut les droits au Tableau de bord de diagnostic de façon à pouvoir accéder aux boutons suivants du Tableau de bord des applications pour le suivi des transactions de l'agent JBoss. Sinon, ces boutons sont désactivés pour ces utilisateurs dans le Tableau de bord des applications.
      1) Le bouton d'analyse détaillée **Diagnostiquer** sur le widget **Slowest 5 Response Time** (Temps de réponse - les 5 les plus lents).
      2) Le bouton **Inflight Requests** sur le widget **Applications**.

   Remarque : La fonction de suivi des transactions est disponible pour l'agent JBoss dans l'offre Cloud APM, Advanced. Pour l'agent JBoss avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez cette étape.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Activer les connexions au serveur JMX MBean

Avant que l'agent JBoss puisse recueillir des données à partir du serveur JBoss, il faut que les connexions au serveur MBean Java Management Extensions (JMX) soient activées.

Procédure

Suivez les étapes correspondant à votre édition et version du serveur JBoss.

- Configurez EAP 5.2.

  Effectuez une copie de sauvegarde du fichier `run.conf`, puis ajoutez-y les lignes suivantes :

  ```
  JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.authenticate=false"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=1090"
  JAVA_OPTS="$JAVA_OPTS -Djavax.management.builder.initial=
                        org.jboss.system.server.jmx.MBeanServerBuilderImpl"
  ```

- Configurez AS 6.x.

  Indiquez l'adresse d'association comme paramètre lorsque vous démarrez le serveur JBoss.

  – Linux *rép_principal_serveur_jboss*`/bin/run.sh -b adresse_IP`

  – Windows *rép_principal_serveur_jboss*`\bin\run.bat -b <adresse_IP>`

  où *rép_principal_serveur_jboss* représente le répertoire d'installation du serveur JBoss.

  Par exemple, si l'adresse d'association est 10.77.9.250 :

  `/apps/wildfly-9.0.2.Final/bin/run.sh -b 10.77.9.250`

- Configurez toutes les autres versions prises en charge.

  Les serveurs JBoss et WildFly sont installés avec leurs ports JMX désactivés pour la gestion à distance par défaut. Vous devez modifier la configuration du serveur JBoss pour autoriser la gestion à distance. Vous devez éditer le fichier *rép_principal_serveur_jboss*`/standalone/configuration/standalone.xml` pour autoriser la gestion à distance.

  1. Effectuez une copie de sauvegarde du fichier *rép_principal_serveur_jboss*`/standalone/configuration/standalone.xml`.

     Où *rép_principal_serveur_jboss* représente le répertoire d'installation du serveur JBoss.

  2. Autorisez la configuration à distance.

     Recherchez `urn:jboss:domain:jmx` et dans la section subsystem, vérifiez que l'entrée `remoting-connector` contient `use-management-endpoint="true"`.

     Exemple de résultat.

     ```
     <subsystem xmlns="urn:jboss:domain:jmx:1.3">
                <expose-resolved-model/>
                <expose-expression-model/>
                <remoting-connector use-management-endpoint="true"/>
     </subsystem>
     ```

  3. Autorisez les connexions à distance.

     Trouvez où les interfaces sont définies et remplacez 127.0.0.1 (bouclage) par l'IP externe sur le serveur avec lequel la connexion doit s'effectuer. Ne pas définir de connexion à 0.0.0.0.

Exemple avant remplacement.

```
<interfaces>
      <interface name="management">
          <inet-address value="${jboss.bind.address.management:127.0.0.1}"/>
      </interface>
      <interface name="public">
          <inet-address value="${jboss.bind.address:127.0.0.1}"/>
      </interface>
...
```

Exemple après remplacement si l'adresse IP externe est 192.168.101.1.

```
<interfaces>
      <interface name="management">
          <inet-address value="${jboss.bind.address.management:192.168.101.1}"/>
      </interface>
      <interface name="public">
          <inet-address value="${jboss.bind.address:192.168.101.1}"/>
      </interface>
...
```

Ajout d'un utilisateur de gestion de serveur JBoss

Avant que l'agent JBoss puisse recueillir des données à partir du serveur JBoss, un utilisateur de gestion doit être ajouté s'il n'en existe pas déjà un.

Procédure

Utilisez le script JBoss **add-user** pour ajouter un utilisateur de gestion.

1. Accédez au répertoire binaire ou `bin` sous le répertoire d'installation du serveur JBoss.
2. Exécutez le script **add-user**.
   - Linux **./add-user.sh**
   - Windows **add-user.bat**
3. Suivez les invites pour générer un utilisateur de gestion.

Exemple

```
root@jboss-wf10-rh7:/apps/wildfly-10.0.0.Final/bin
] ./add-user.sh

Quel type d'utilisateur souhaitez-vous ajouter ?
 a) Utilisateur de gestion (mgmt-users.properties)
 b) Utilisateur d'application (application-users.properties)
(a) : a

Entrez les détails du nouvel utilisateur à ajouter.
Utilisez le domaine 'ManagementRealm' tel qu'il a été découvert à partir des fichiers de propriétés existants.
Nom d'utilisateur : MyAdmin
Les recommandations relatives au mot de passe sont indiquées ci-dessous. Pour modifier ces restrictions, modifiez le fichie
.
 - Le mot de passe doit être différent du nom d'utilisateur.
 - Le mot de passe ne doit pas être l'une des valeurs restreintes suivantes {root, admin, administrateur}
 - Le mot de passe doit contenir au moins 8 caractères, 1 caractère alphabétique, 1 caractère numérique,
1 symbole non alphanumérique
Mot de passe :
Entrer à nouveau le mot de passe :
A quel groupe souhaitez-vous que cet utilisateur appartienne ? (Veuillez entrer une liste séparée par des virgules, ou lais
pour n'en indiquer aucun)[  ] :
En ce qui concerne l'ajout de l'utilisateur 'MyAdmin' pour le domaine 'ManagementRealm'
Est-ce correct, oui/non ? oui
Utilisateur 'MyAdmin' ajouté au fichier '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-users.properties'
Utilisateur 'MyAdmin' ajouté au fichier '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-users.properties'
Utilisateur 'MyAdmin' ajouté avec des groupes au fichier
          '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-groups.properties'
```

```
Utilisateur 'MyAdmin' ajouté avec des groupes au fichier
          '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-groups.properties'
Ce nouvel utilisateur va-t-il être utilisé pour qu'un processus AS se connecte à un autre processus AS ?
Par exemple, pour qu'un contrôleur d'hôte esclave se connecte au maître ou pour l'exécution d'une connexion à distance pa
à serveur.
oui/non ? non
```

Activation de la collecte des statistiques Web/HTTP

Avant que l'agent JBoss ne puisse recueillir les mesures Web du serveur JBoss et les mesures des autres sous-systèmes, la collecte des statistiques doit être activée pour chaque sous-système. Cette procédure est applicable à JBoss EAP version 7.x et WildFly versions 8.x, 9.x et 10.x.

Procédure

L'attribut **statistics-enabled** des divers sous-systèmes JBoss contrôle la collecte des statistiques. Il peut être affiché et mis à jour à l'aide de l'interface de ligne de commande JBoss.

Remarque : Cette procédure est applicable à JBoss EAP version 7.x et WildFly versions 8.x, 9.x et 10.x.

1. Accédez au répertoire binaire ou `bin` sous le répertoire d'installation du serveur JBoss.
2. Démarrez l'interface de ligne de commande JBoss.
   - Linux **./jboss-cli.sh --connect** [**--controller**=*IP*:*port*]
   - Windows **jboss-cli.bat --connect** [**--controller**=*IP*:*port*]

   où *IP* représente l'adresse IP du serveur JBoss et *port*, le port du serveur JBoss. Par exemple, `192.168.10.20:9990`.

   Conseil : si la tentative de connexion se solde par un échec, "`Echec de la connexion au contrôleur : Le contrôleur n'est pas disponible à localhost:9990. La connexion a échoué : WFLYPRT0053 : Echec de la connexion à http-remoting://localhost:9990. Echec de la connexion : Connexion refusée`", utilisez le paramètre **--controller**.

   Cette erreur indique que le serveur de gestion n'est pas en mode écoute sur l'adresse IP du système hôte local (127.0.0.1) et qu'il est configuré pour être en mode écoute sur l'adresse IP de l'ordinateur.
3. Exécutez les commandes suivantes pour afficher l'état actuel de l'attribut statistics-enabled de chaque sous-système :

   `/subsystem=`**`ejb3`**`:read-attribute(name=enable-statistics)`

   `/subsystem=`**`transactions`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`undertow`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`webservices`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nom_Source_Données`*`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nom_Source_Données`*`/`**`statistics=pool`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nom_Source_Données`*`/`**`statistics=jdbc`**`:read-attribute(name=statistics-enabled)`

   où *Nom_Source_Données* représente le nom d'une source de données configurée pour être utilisée avec JBoss.

   Remarque : les sources de données peuvent être répertoriées à l'aide de la commande `/subsystem=datasources:read-resource`.
   Exemple de résultat lorsque les statistiques ne sont pas activées :

```
{
    "outcome" => "success",
    "result" => false
}
```

4. Exécutez la commande suivante pour remplacer la valeur de l'attribut statistics-enabled de chaque sous-système par *true* :

   ```
   /subsystem=ejb3:write-attribute(name=enable-statistics, value=true)
   ```

   ```
   /subsystem=transactions:write-attribute(name=statistics-enabled,value=true)
   ```

   ```
   /subsystem=undertow:write-attribute(name=statistics-enabled,value=true)
   ```

   ```
   /subsystem=webservices:write-attribute(name=statistics-enabled,value=true)
   ```

   ```
   /subsystem=datasources/data-source=Nom_Source_Données:write-attribute(name=statistics-enabled,value=true)
   ```

   ```
   /subsystem=datasources/data-source=Nom_Source_Données/statistics=pool:write-attribute(name=statistics-enabled,value=true)
   ```

   ```
   /subsystem=datasources/data-source=Nom_Source_Données/statistics=jdbc:write-attribute(name=statistics-enabled,value=true)
   ```

   Exemple de résultat lorsque vous activez les statistiques d'un sous-système :

   ```
   {
       "outcome" => "success",
       "response-headers" => {
           "operation-requires-reload" => true,
           "process-state" => "reload-required"
       }
   }
   ```

5. Quittez l'interface de ligne de commande JBoss.
6. Redémarrez le serveur JBoss.

   Remarque : Les agents JBoss en cours d'exécution avec le suivi des transactions activé doivent être redémarrés.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent JBoss sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for JBoss**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `jboss01`.

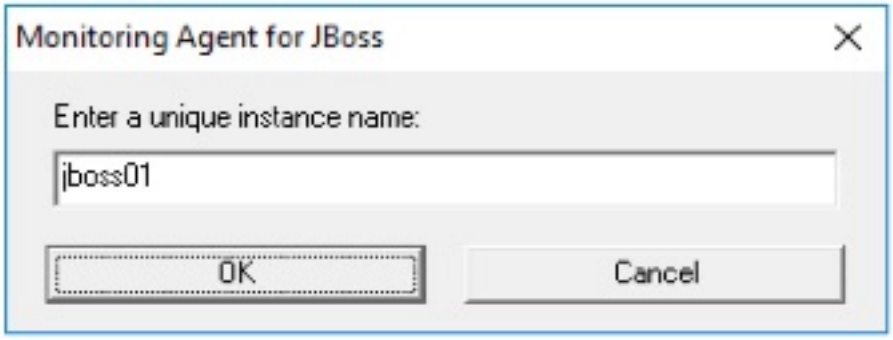


Figure 17. Fenêtre de saisie d'un nom d'instance unique.

4. Entrez les paramètres du serveur JBoss, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 123, à la page 433.

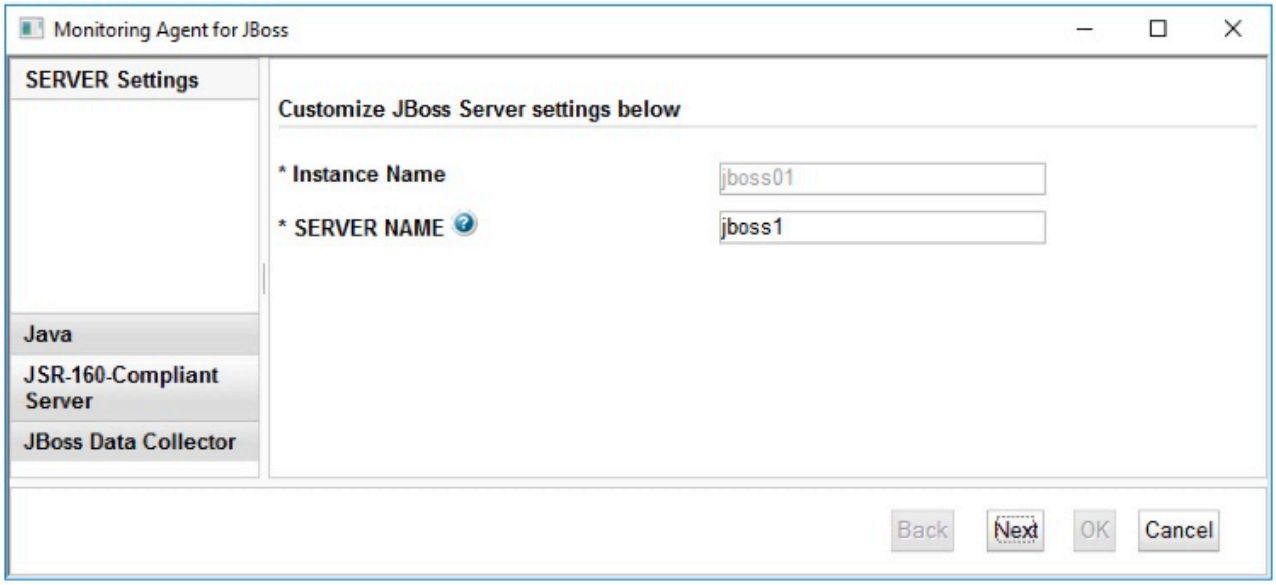


Figure 18. Fenêtre des paramètres de configuration pour le serveur JBoss

5. Entrez les paramètres Java, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 123, à la page 433.

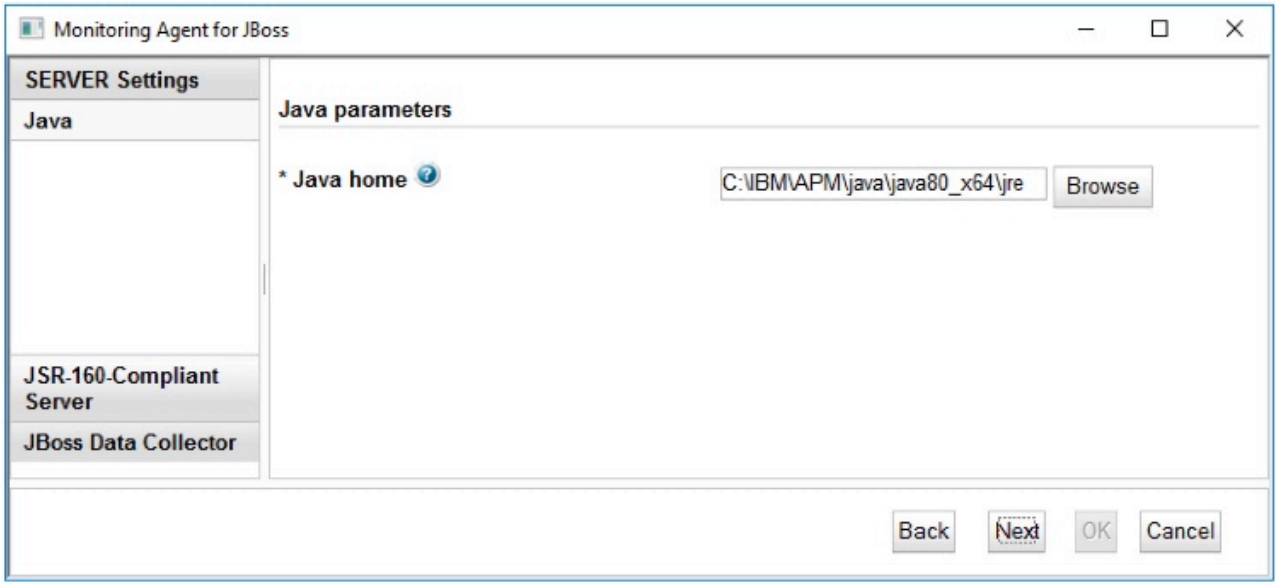


Figure 19. Fenêtre de spécification des paramètres Java.

6. Entrez les paramètres JMX, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 123, à la page 433.

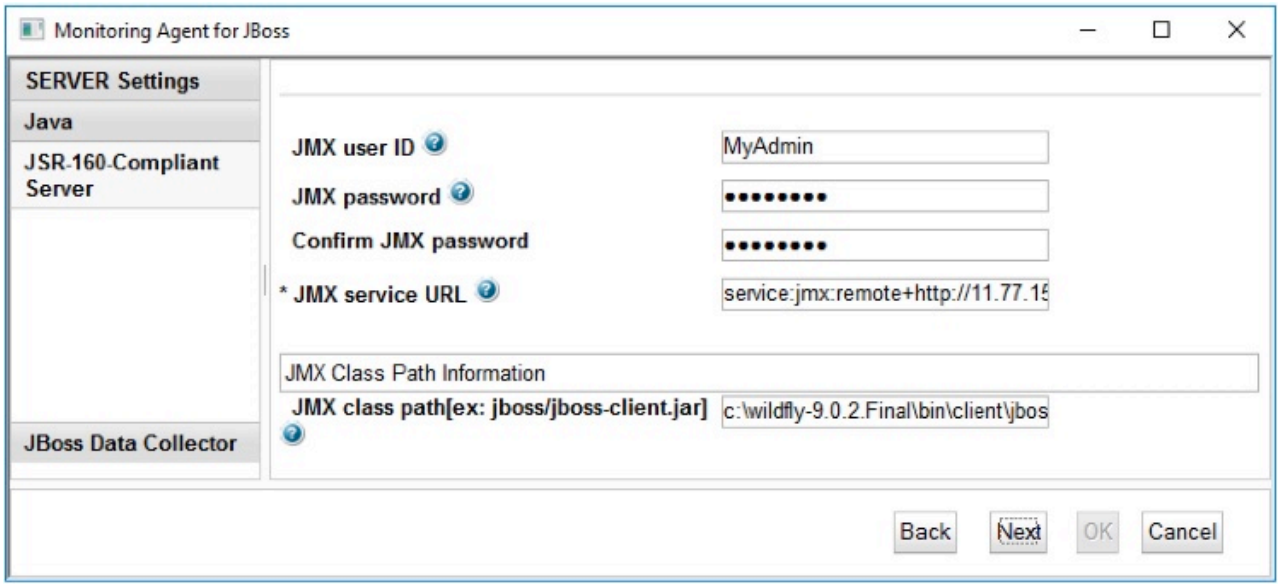


Figure 20. Fenêtre de spécification des paramètres JMX.

7. Affichez les paramètres du collecteur de données d'agent de l'agent JBoss. Laissez le paramètre **DC Runtime Directory** vide lors de la configuration initiale de l'agent. Pour obtenir une description de chaque paramètre de configuration, voir tableau 123, à la page 433.

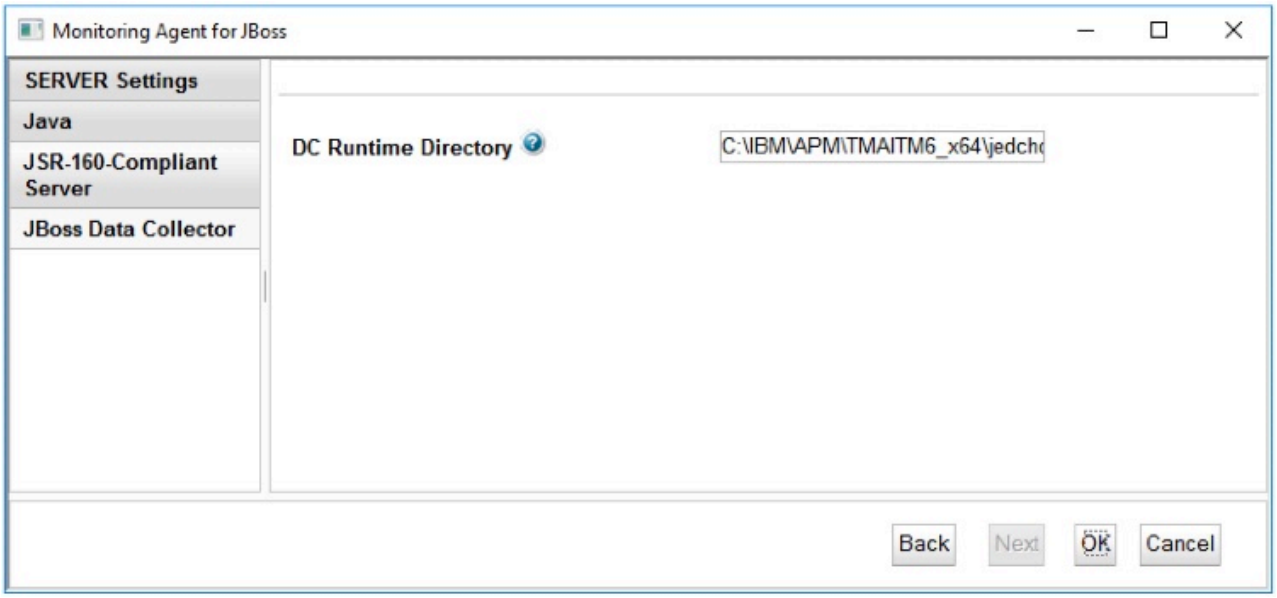


Figure 21. Fenêtre de spécification des paramètres du collecteur de données de l'agent JBoss.

8. Cliquez sur **OK** pour terminer la configuration de l'agent.
9. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent JBoss, vous devez le configurer pour pouvoir le démarrer. Si l'agent JBoss est installé sur un ordinateur Linux ou UNIX local, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

1. A partir d'une ligne de commande, exécutez la commande suivante :

   ```
   rép_install/bin/jboss-agent.sh config
   nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent JBoss», à la page 433.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/jboss-agent.sh start
   nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
   ```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent JBoss en mode silencieux, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier `jboss_silent_config.txt` disponible à l'emplacement suivant :
   - Linux AIX *rép_install*`/samples/jboss_silent_config.txt`
     Par exemple, `/opt/ibm/apm/agent/samples/jboss_silent_config.txt`
   - Windows *rép_install*`\samples\jboss_silent_config.txt`

   où *rép_install* représente le chemin d'installation de l'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM\TMAITM6_x64`

   Exemple Linux AIX

   ```
   /opt/ibm/apm/agent/samples/jboss_silent_config.txt
   ```

   Windows

   ```
   C:\IBM\APM\samples\jboss_silent_config.txt
   ```
2. Dans le fichier `jboss_silent_config.txt`, indiquez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent JBoss», à la page 433.
3. Sauvegardez et fermez le fichier `jboss_silent_config.txt`, puis exécutez la commande suivante :
   - Linux AIX *rép_install*`/bin/jboss-agent.sh config` **`nom_instance`** *rép_install*`/samples/jboss_silent_config.txt`
   - Windows *rép_install*`\bin\jboss-agent.bat config` **`nom_instance`** *rép_install*`\samples\jboss_silent_config.txt`

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM\TMAITM6_x64`

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

Exemple Linux AIX

```
/opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows

```
C:\IBM\APM\bin\jboss-agent.bat config example-inst01 C:\IBM\APM\samples\jboss_silent_config.txt
```

4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux AIX *rép_install*/bin/jboss-agent.sh start **nom_instance**
   - Windows *rép_install*\bin\jboss-agent.bat start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM\TMAITM6_x64`

   Exemple Linux AIX

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
   ```

   Windows

   ```
   C:\IBM\APM\bin\jboss-agent.bat start example-inst01
   ```

Paramètres de configuration de l'agent JBoss

Les paramètres de configuration de l'agent JBoss sont regroupés dans un tableau.

1. Paramètres de l'agent JBoss - Paramètres de l'environnement de l'agent JBoss.
2. tableau 124, à la page 434 - Exemples d'adresses URL de service de JMX.

Tableau 123. Paramètres de l'agent JBoss

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
nom de serveur	Indiquez un nom pour identifier le serveur JBoss/WildFly.	**KJE_SERVER**
Accueil Java	Chemin d'accès où Java est installé.	**JAVA_HOME**
ID utilisateur JMX	ID utilisateur pour la connexion au serveur MBean.	**KQZ_JMX_JSR160_JSR160_USER_ID**
Mot de passe JMX	Mot de passe	**KQZ_JMX_JSR160_JSR160_PASSWORD**
Adresse URL de service JMX	Adresse URL de service pour la connexion au serveur MBean. Voir tableau 124, à la page 434 pour obtenir des exemples.	**KQZ_JMX_JSR160_JSR160_SERVICE_URL**
Chemin d'accès aux classes JMX	Fichiers JAR dans lesquels sont recherchées les localisations d'une classe ou d'une ressource. Localisez et entrez le chemin d'accès au fichier `jboss-client.jar` pour votre serveur JBoss. Exemple pour un serveur JBoss EAP 6 : `/opt/EAP-6.3.0/jboss-eap-6.3/bin/client/jboss-client.jar`.	**KQZ_JMX_JSR160_JSR160_JAR_FILES**

Tableau 123. Paramètres de l'agent JBoss (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Répertoire d'exécution DC	**Remarque :** Ce paramètre concerne uniquement l'agent JBoss avec la fonction de suivi des transactions, qui fait partie de l'offre de Cloud APM, Advanced. Pour l'agent JBoss avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez ce paramètre. Le chemin d'accès complet au répertoire d'exécution du collecteur de données JBoss est défini par le script **simpleConfig**. Laissez ce paramètre vide lors de la configuration initiale de l'agent.	**KQZ_DC_RUNTIME_DIR**

Tableau 124. Adresse URL de service JMX

Version du serveur JBoss	Adresse URL de service JMX avec un port par défaut[1]
WildFly 8, 9 et 10 JBoss EAP 7	`service:jmx:remote+http://ip:9990` `service:jmx:remote+https://ip:9994`
JBoss EAP 6 JBoss AS 7	`service:jmx:remoting-jmx://ip:9999`
JBoss EAP 5.2 JBoss AS 6.1	`service:jmx:rmi:///jndi/rmi://ip:1090/jmxrmi`

[1] Le port est défini en fonction du port contenu dans l'entrée suivante du fichier de configuration de JBoss : `<socket-binding name="management-native" interface="management" port="${jboss.management.native.port:NNNN}"/>`. Si la valeur par défaut du port a été modifiée, redéfinissez-la sur le numéro de port contenu dans votre fichier de configuration.

Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss

La fonction de suivi des transactions de l'agent JBoss requiert des modifications dans le fichier des paramètres d'environnement de l'instance d'agent, le fichier de démarrage du serveur JBoss et le paramètre de configuration de l'agent DC Runtime Directory. Un script est fourni pour vous aider à apporter ces modifications.

Avant de commencer

Linux Vérifiez que la limite de ressource pour les fichiers ouverts est supérieure à 5 000 pour que le kit d'outils de suivi des transactions fonctionne correctement.

- Affichez le paramètre de limite de fichiers ouverts en cours. **ulimit -n**
- Exemple de paramètre définissant la limite de fichiers ouverts à 5 056. **ulimit -n 5056**

Effectuez l'étape Configuration de l'agent JBoss 1, à la page 424 ou 2, à la page 424 avant de suivre cette procédure.

L'agent JBoss doit être installé en local sur le serveur JBoss surveillé avec la fonction de suivi des transactions.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *JBOSS_HOME*.
2. Répertoire *JBOSS_HOME*/bin et ses fichiers.
3. Fichier *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml.
4. Répertoire *rép_install*/config.
5. Fichier *rép_install*/config/*nom_hôte*_je_*nom_instance*.cfg.

où

JBOSS_HOME
Répertoire d'installation du serveur JBoss.

rép_install
Chemin d'installation de l'agent. Le chemin d'accès par défaut est :

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

nom_hôte
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 428
- Configuration de l'agent en répondant à des invites, étape 1, à la page 431
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 3, à la page 432

Procédure

Exécutez le script **simpleConfig**.

1. Connectez-vous au serveur JBoss sur lequel l'agent JBoss est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux *rép_install*
   - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
3. Accédez au répertoire jedchome/7.3.0.13.0/bin.
4. Exécutez le script d'installation.
   - Linux ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Suivez les invites pour entrer des paramètres pour votre environnement :
   a. Entrez le *nom_instance* de l'agent JBoss choisi pour l'instance d'agent.
   b. Entrez le répertoire d'installation du serveur JBoss. Si la variable d'environnement *JBOSS_HOME* est définie, sa valeur sera proposée comme valeur par défaut.

   où

   JBOSS_HOME
   Répertoire d'installation du serveur JBoss.

   nom_instance
   Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 428
- Configuration de l'agent en répondant à des invites, étape 1, à la page 431
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 3, à la page 432

rép_install
Chemin où l'agent est installé. Le chemin d'accès par défaut est :
- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

6. Redémarrez l'agent et le serveur JBoss s'ils sont en cours d'exécution.

Résultats

Fichiers du serveur JBoss modifiés lors de la configuration du suivi des transactions :

- *JBOSS_HOME*`/bin/standalone.conf`
  Ce fichier est mis à jour avec les paramètres de configuration requis pour la fonction de suivi des transactions. Des repères de configuration sont insérés dans le fichier pour pouvoir être utilisés lorsque vous désactivez la fonction de suivi des transactions. Un fichier de sauvegarde est sauvegardé dans le répertoire *JBOSS_HOME*`/bak` avant l'ajout ou la suppression de modifications de la fonction de suivi des transactions.
- *JBOSS_HOME*`/modules/system/layers/base/org/jboss/as/server/main/module.xml`
  Ce fichier est mis à jour avec une dépendance de module d'API JAVA EE. Des repères de configuration sont insérés dans le fichier pour pouvoir être utilisés lorsque vous désactivez la fonction de suivi des transactions. Un fichier de sauvegarde est sauvegardé dans le répertoire *JBOSS_HOME*`/bak` avant l'ajout ou la suppression de modifications de la fonction de suivi des transactions.

Fichiers de l'agent modifiés lors de la configuration du suivi des transactions :

- Fichier de configuration de l'instance d'agent
  - Linux *rép_install*`/config/`*nom_hôte*`_je_`*nom_instance*`.cfg`
  - Windows *rép_install*`\TMAITM6_x64\`*nom_hôte*`_JE_`*nom_instance*`.cfg`
- Fichier des paramètres d'environnement de l'agent
  - Linux *rép_install*`/config/je_`*nom_instance*`.environment`
  - Windows *rép_install*`\TMAITM6_x64\KJEENV_`*nom_instance*

où

JBOSS_HOME
Répertoire d'installation du serveur JBoss.

rép_install
Chemin d'installation de l'agent. Le chemin d'accès par défaut est :
- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nom_hôte
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :
- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 428
- Configuration de l'agent en répondant à des invites, étape 1, à la page 431
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 3, à la page 432

Désactivation du collecteur de données du suivi des transactions de l'agent JBoss

La fonction de suivi des transactions de l'agent JBoss requiert des modifications dans le fichier des paramètres d'environnement de l'instance d'agent, le fichier de démarrage du serveur JBoss et le paramètre de configuration de l'agent DC Runtime Directory. Un script est fourni pour supprimer ces modifications pour une instance d'agent dont le suivi des transactions est activé.

Avant de commencer

Assurez-vous que le serveur JBoss et l'agent JBoss sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *JBOSS_HOME*.
2. Répertoire *JBOSS_HOME*/bin et ses fichiers.
3. Fichier *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml.
4. Répertoire *rép_install*/config.
5. Fichier *rép_install*/config/*nom_hôte*_je_*nom_instance*.cfg.

Procédure

Exécutez le script **simpleConfig** avec l'option **remove**.

1. Connectez-vous au serveur JBoss sur lequel l'agent JBoss est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux *rép_install*
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire jedchome/7.3.0.13.0/bin.
4. Exécutez le script **simpleConfig** avec l'option **remove**.
   - Linux ./simpleConfig.sh **remove** *nom_instance*
   - Windows simpleConfig.bat **remove** *nom_instance*
5. Démarrez l'agent et le serveur JBoss.

   Où :

   JBOSS_HOME
   Répertoire d'installation du serveur JBoss.

   nom_hôte
   Nom de l'ordinateur hôte sur lequel l'agent est installé.

   nom_instance
   Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :
   - Configuration de l'agent sur des systèmes Windows, étape 3, à la page 428
   - Configuration de l'agent en répondant à des invites, étape 1, à la page 431
   - Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 3, à la page 432

   rép_install
   Chemin où l'agent est installé. Le chemin d'accès par défaut est :
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   architecture
   Identificateur de l'architecture système d'IBM Application Performance Management ou de

Cloud APM. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install*/registry/archdsc.tbl.

Désinstallation du suivi des transactions de tous les agents JBoss

La fonction de suivi des transactions de l'agent JBoss peut être désinstallée. Un script est fourni pour supprimer toutes les instances d'agent dont le suivi des transactions est activé et le kit d'outils du suivi des transactions.

Avant de commencer

Assurez-vous que le serveur JBoss et toutes les instances d'agent JBoss sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits d'accès en écriture aux répertoires et fichiers suivants :

1. Répertoire *JBOSS_HOME*.
2. Répertoire *JBOSS_HOME*/bin et ses fichiers.
3. Fichier *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml.
4. Répertoire *rép_install*/config.
5. Fichier *rép_install*/config/*nom_hôte*_je_*nom_instance*.cfg.

Procédure

Exécutez le script **simpleConfig** avec l'option **uninstall**.

1. Connectez-vous au serveur JBoss sur lequel l'agent JBoss est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux *rép_install*/*architecture*/je/bin. Par exemple : /opt/ibm/apm/agent/lx8266/je/bin ou /opt/ibm/apm/agent/lx8266/je/bin
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire jedchome/7.3.0.13.0/bin.
4. Exécutez le script **simpleConfig** avec l'option **uninstall**.
   - Linux ./simpleConfig.sh **uninstall**
   - Windows simpleConfig.bat **uninstall**
5. Démarrez le serveur JBoss et toutes les instances d'agent.

Où :

JBOSS_HOME
Répertoire d'installation du serveur JBoss.

nom_hôte
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 428
- Configuration de l'agent en répondant à des invites, étape 1, à la page 431
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 3, à la page 432

rép_install
Chemin où l'agent est installé. Le chemin d'accès par défaut est :

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

architecture
Identificateur de l'architecture système d'IBM Application Performance Management ou de Cloud APM. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install*/registry/archdsc.tbl.

Configuration de la surveillance de Linux KVM

Vous devez configurer l'Monitoring Agent for Linux KVM pour collecter les données des serveurs Red Hat Enterprise Virtualization Hypervisor (RHEVH) et Red Hat Enterprise Virtualization Manager (RHEVM). Une fois que vous avez installé l'agent sur un serveur ou une machine virtuelle, vous devez créer la première instance et démarrer l'agent manuellement.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Linux KVM.

Pourquoi et quand exécuter cette tâche

L'Agent Linux KVM est un agent multi-instance et à connexions multiples. Multi-instance signifie que vous pouvez créer plusieurs instances et que chaque instance peut établir plusieurs connexions à un ou plusieurs serveurs RHEVM ou RHEVH.

A faire : Utilisez des instances différentes pour surveiller les serveurs RHEVM ou RHEVH.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 125. Versions d'agent et documentation

Version de l'Agent Linux KVM	Documentation
7.2.1.6	IBM Cloud Application Performance Management
7.2.1.5, 7.2.1.4	IBM Performance Management 8.1.3 *
7.2.1.3	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Vous pouvez utiliser le même script de configuration afin de configurer des instances pour les serveurs RHEVH et RHEVM :

- Pour configurer une connexion au serveur de RHEVM, effectuez les étapes décrites dans la section «Configuration d'une connexion au serveur RHEVM».
- Pour configurer une connexion au serveur de RHEVH, effectuez les étapes décrites dans la section «Configuration d'une connexion au serveur RHEVH».

Création d'un utilisateur et attribution des droits nécessaires

Avant de configurer l'Agent Linux KVM, vous devez créer un utilisateur et lui accorder les droits appropriés lui permettant de surveiller les serveurs RHEVM et RHEVH.

Procédure

1. Ouvrez le portail **Red Hat Enterprise Virtualization Manager Web Administration**.
2. Cliquez sur **Configure**.

3. Dans la fenêtre Configuration, sélectionnez **Roles**.
   a. Pour créer un rôle, cliquez sur **Nouveau**.
   b. Dans la fenêtre New role, ajoutez le nom du rôle et sélectionnez **Admin** comme type de compte.
   c. Assurez-vous que les cases à cocher du panneau Check boxes to Allow Action ne sont pas sélectionnées, et cliquez sur **OK**.
4. Dans la fenêtre Configuration, sélectionnez **System Permission**.
   a. Pour accorder un droit utilisateur, cliquez sur **Add**.
   b. Dans la fenêtre Add System Permission to User, sélectionnez l'utilisateur auquel vous souhaitez accorder le droit.
   c. Dans la liste **Assign role to user**, sélectionnez le rôle que vous avez créé et cliquez sur **OK**.

Que faire ensuite

Effectuez la configuration de l'agent :

- «Configuration d'une connexion au serveur RHEVH», à la page 446
- «Configuration d'une connexion au serveur RHEVM», à la page 444

Configuration des protocoles

L'agent utilise différents protocoles pour la connexion au serveur RHEVH. Vous pouvez configurer l'un de ces protocoles : SSH, TLS ou TCP.

Pourquoi et quand exécuter cette tâche

L'Agent Linux KVM se connecte à distance à chaque hyperviseur à l'aide de l'outil **virsh** qui gère vos machines virtuelles QEMU-KVM, et il collecte les mesures. L'API `libvirt` de l'environnement d'agent utilise plusieurs protocoles de transport à distance différents. Pour obtenir la liste des protocoles pris en charge, voir la Remote support page (page de support à distance).

Configuration du protocole SSH

Vous pouvez configurer le protocole SSH pour surveiller un hôte à distance.

Pourquoi et quand exécuter cette tâche

Supposition : L'Agent Linux KVM est installé sur l'hôte A. Vous souhaitez surveiller à distance l'hyperviseur sur l'hôte B.

Procédure

1. Connectez-vous à l'hôte A en utilisant le même ID utilisateur que celui avec lequel le processus de l'Agent Linux KVM est exécuté, par exemple, l'ID du superutilisateur.

   Conseil : Assurez-vous de connaître l'ID sur l'hôte B qui accepte la connexion SSH, ainsi que l'ID du superutilisateur sur l'hôte A.
2. Générez les clés **id_rsa** et **id_rsa.pub** sur l'hôte A à l'aide de l'utilitaire *ssh-keygen*. Les clés sont sauvegardées à l'emplacement : `~/.ssh: $ ssh-keygen -t rsa`.
3. Copiez les clés autorisées à partir de l'hôte B :

   ```
   $ scp Id on host B@name or IP address of host B:~/.ssh/authorized_keys ~/.ssh/
   authorized_keys_from_B
   ```
4. Ajoutez la clé publique pour l'hôte A à la fin des clés autorisées pour l'hôte B :

   ```
   cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys_from_B
   ```
5. Copiez les clés autorisées vers l'hôte B :

```
$ scp ~/.ssh/authorized_keys_from_B Id on host B@name or IP address of host
B:~/.ssh/authorizede_keys
```

A faire : Si vous surveillez plusieurs hôtes, répétez les étapes 3, à la page 440, 4, à la page 440 et 5, à la page 440 pour chaque hôte.

6. Supprimez les clés autorisées que vous avez copiées sur l'hôte B :

   ```
   ~/.ssh/authorized_keys_from_B
   ```

7. Ajoutez la commande suivante au profil **~/.bash_** de l'ID en cours sur l'hôte A :

   ```
   $ eval `ssh-agent`
   ```

   A faire : Veillez à utiliser l'apostrophe inversée (`) qui se trouve sur la touche de la lettre è (pour l'obtenir : AltGR + touche è) du clavier français, et non le guillemet simple (').

8. Ajoutez l'identité à l'hôte A et entrez le mot de passe que vous avez utilisé pour créer l'ID :

   ```
   $ ssh-add ~/.ssh/id_rsa
   ```

9. Exécutez la commande suivante si vous recevez le message `Could not open a connection to your authentication agent` :

   ```
   exec ssh-agent bash
   ```

   Conseil : Vous pouvez remplacer l'interpréteur de commandes bash par l'interpréteur de commandes que vous utilisez, puis exécuter à nouveau la commande suivante :

   ```
   $ ssh-add ~/.ssh/id_rsa
   ```

10. Testez le protocole SSH pour vérifier qu'il parvient à se connecter de l'hôte A à l'hôte B sans qu'il soit nécessaire d'entrer le mot de passe SSH :

    Conseil : Si vous surveillez plusieurs hôtes, utilisez la commande suivante pour tester la connexion pour chacun d'eux :

    ```
    $ ssh Id on host B@name or IP address of host B
    ```

11. Pour vérifier la connexion, exécutez la commande suivante :

    ```
    virsh -c qemu+ssh://Id on host B@name or IP address of host B:port/system
    ```

    Si vous n'avez pas modifié le port SSH par défaut, omettez la section **:port** dans la commande.

    Important : Si la commande **virsh** aboutit, l'Agent Linux KVM se connecte à l'hyperviseur.

12. Vous devez redémarrer l'hôte A avant de redémarrer l'Agent Linux KVM sur l'hôte A. Pour cela, exécutez à nouveau la commande **ssh-add** et indiquez le mot de passe à chaque fois.

    Conseil : Vous pouvez utiliser des chaînes de clés SSH pour éviter d'avoir à ressaisir le mot de passe.

Configuration du protocole TLS

Vous pouvez configurer le protocole TLS pour surveiller un hôte à distance.

Pourquoi et quand exécuter cette tâche

Supposition : L'Agent Linux KVM est installé sur l'hôte A. Vous souhaitez surveiller à distance l'hyperviseur sur l'hôte B.

Procédure

1. Pour créer une clé de l'autorité de certification (CA) et un certificat dans votre hyperviseur, effectuez les étapes suivantes :
   a. Connectez-vous à l'hôte B.

b. Créez un répertoire temporaire et modifiez le chemin d'accès en fonction de ce répertoire temporaire :

```
mkdir fichiers_cert
cd fichiers_cert
```

c. Créez une clé RSA de 2048 bits :

```
openssl genrsa -out cakey.pem 2048
```

d. Créez un certificat autosigné pour votre autorité de certification locale :

```
openssl req -new -x509 -days 1095 -key cakey.pem -out \
cacert.pem -sha256 -subj "/C=US/L=Austin/O=IBM/CN=my CA"
```

e. Vérifiez votre certificat de l'autorité de certification :

```
openssl x509 -noout -text -in cacert.pem
```

2. Pour créer les clés et certificats du client et du serveur dans votre hyperviseur, effectuez les étapes suivantes :

a. Créez les clés :

```
openssl genrsa -out serverkey.pem 2048
openssl genrsa -out clientkey.pem 2048
```

b. Créez une demande de signature de certificat pour le serveur :

A faire : Remplacez l'adresse kvmhost.company.org, qui est utilisée dans la demande de certificat de serveur, par le nom de domaine complet de votre hôte d'hyperviseur.

```
openssl req -new -key serverkey.pem -out serverkey.csr \
-subj "/C=US/O=IBM/CN=kvmhost.company.org"
```

c. Créez une demande de signature de certificat pour le client :

```
openssl req -new -key clientkey.pem -out clientkey.csr \
-subj "/C=US/O=IBM/OU=virtualization/CN=root"
```

d. Créez les certificats client et serveur :

```
openssl x509 -req -days 365 -in clientkey.csr -CA cacert.pem \
-CAkey cakey.pem -set_serial 1 -out clientcert.pem
openssl x509 -req -days 365 -in serverkey.csr -CA cacert.pem \
-CAkey cakey.pem -set_serial 94345 -out servercert.pem
```

e. Vérifiez les clés :

```
openssl rsa -noout -text -in clientkey.pem
openssl rsa -noout -text -in serverkey.pem
```

f. Vérifiez les certificats :

```
openssl x509 -noout -text -in clientcert.pem
openssl x509 -noout -text -in servercert.pem
```

3. Pour distribuer les clés et les certificats au serveur hôte, effectuez les étapes suivantes :

a. Copiez le fichier `cacert.pem` du certificat de l'autorité de certification dans ce répertoire : `/etc/pki/CA`

```
cp cacert.pem /etc/pki/CA/cacert.pem
```

b. Créez le répertoire `/etc/pki/libvirt` et copiez le fichier de certificat de serveur `servercert.pem` dans le répertoire `/etc/pki/libvirt`. Assurez-vous que seul le superutilisateur peut accéder à la clé privée.

```
mkdir /etc/pki/libvirt
cp servercert.pem /etc/pki/libvirt/.
chmod -R o-rwx /etc/pki/libvirt
```

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

c. Créez le répertoire `/etc/pki/libvirt/private` et copiez le fichier de clés serveur `serverkey.pem` dans le répertoire `/etc/pki/libvirt/private`. Assurez-vous que seul le superutilisateur peut accéder à la clé privée.

```
mkdir /etc/pki/libvirt/private
cp serverkey.pem /etc/pki/libvirt/private/.
chmod -R o-rwx /etc/pki/libvirt/private
```

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

d. Vérifiez que les fichiers sont placés correctement :

```
find /etc/pki/CA/*|xargs ls -l
ls -lR /etc/pki/libvirt
ls -lR /etc/pki/libvirt/private
```

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

4. Pour distribuer les clés et les certificats aux clients ou aux stations de gestion, effectuez les étapes suivantes :
   a. Connectez-vous à l'hôte A.
   b. Copiez le certificat de l'autorité de certification `cacert.pem` de l'hôte dans le répertoire `/etc/pki/CA` sur l'hôte A sans changer le nom de fichier.

```
scp kvmhost.company.org:/tmp/cacert.pem /etc/pki/CA/
```

   c. Copiez le fichier `clientcert.pem` de certificat client dans le répertoire `/etc/pki/libvirt` de l'hôte B. Utilisez les noms de fichier par défaut et assurez-vous que seul le superutilisateur peut accéder à la clé privée.

```
mkdir /etc/pki/libvirt/
scp kvmhost.company.org:/tmp/clientcert.pem /etc/pki/libvirt/.
chmod -R o-rwx /etc/pki/libvirt
```

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

   d. Copiez la clé du client `clientkey.pem` dans le répertoire `/etc/pki/libvirt/private` de l'hôte. Utilisez les noms de fichier par défaut et assurez-vous que seul le superutilisateur peut accéder à la clé privée.

```
mkdir /etc/pki/libvirt/private
scp kvmhost.company.org:/tmp/clientkey.pem /etc/pki/libvirt/private/.
chmod -R o-rwx /etc/pki/libvirt/private
```

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

   e. Vérifiez que les fichiers sont placés correctement :

```
ls -lR /etc/pki/libvirt
ls -lR /etc/pki/libvirt/private
```

5. Pour modifier la configuration du démon `libvirtd`, effectuez les étapes suivantes :
   a. Connectez-vous à l'hôte B.
   b. Effectuez une copie du fichier `/etc/sysconfig/libvirtd` et du fichier `/etc/libvirt/libvirtd.conf`.

c. Editez le fichier /etc/sysconfig/libvirtd et assurez-vous que le paramètre **--listen** est transmis au démon libvirtd. Cette étape permet de s'assurer que le démon libvirtd est en mode écoute sur les connexions réseau.

d. Editez le fichier /etc/libvirt/libvirtd.conf et configurez un ensemble de sujets autorisés avec l'instruction **tls_allowed_dn_list** dans le fichier libvirtd.conf.

   Important : Les zones figurant dans le sujet doivent suivre le même ordre que celui que vous avez utilisé pour créer le certificat.

e. Redémarrez le service démon libvirtd pour que les modifications soient prises en compte :

   /etc/init.d/libvirtd restart

6. Pour modifier la configuration du pare-feu, accédez à la configuration du niveau de sécurité et ajoutez le port TCP 16514 comme port sécurisé.
7. Pour vérifier que la gestion à distance fonctionne, exécutez la commande suivante sur l'hôte A :

   virsh -c qemu+tls://kvmhost.company.org/system list --all

Configuration du protocole TCP

Utilisez le protocole TCP uniquement à des fins de test.

Pourquoi et quand exécuter cette tâche

Supposition : L'Agent Linux KVM est installé sur l'hôte A. Vous souhaitez surveiller à distance l'hyperviseur sur l'hôte B.

Procédure

1. Connectez-vous à l'hôte B.
2. Editez le fichier /etc/libvirt/libvirtd.conf et assurez-vous que le paramètre **listen_tcp** est activé, et que le paramètre **tcp_port** est défini sur la valeur par défaut 16509.
3. Editez le fichier /etc/libvirt/libvirtd.conf pour définir le paramètre **auth_tcp** sur «none». Cette étape invite TCP à ne pas authentifier la connexion.
4. Redémarrez le démon **libvirt** sur l'hôte B en mode écoute en l'exécutant avec l'indicateur **--listen** ou en éditant le fichier /etc/sysconfig/libvirtd et en supprimant la mise en commentaire de la ligne LIBVIRTD_ARGS="--listen".
5. Pour vérifier la connexion, exécutez la commande suivante :

   virsh -c qemu+tcp://kvmhost.company.org:port/system

   Si vous n'avez pas modifié le port TCP par défaut, omettez la section **:port** dans la commande.

   Important : Si la commande **virsh** aboutit, l'Agent Linux KVM se connecte à l'hyperviseur.

Que faire ensuite

Configurez l'agent en effectuant les étapes décrites dans «Configuration d'une connexion au serveur RHEVH», à la page 446.

Configuration d'une connexion au serveur RHEVM

Pour configurer une connexion au serveur RHEVM, vous devez exécuter le script et répondre aux invites.

Avant de commencer

1. Téléchargez le certificat de sécurité qui est disponible à l'emplacement suivant :

   https://*HOTE-RHEVM*:*PORT-RHEVM*/ca.crt

   Où

HOTE-RHEVM
Nom de l'hôte.

PORT-RHEVM
Port que vous utilisez dans votre environnement RHEVM.

2. Utilisez l'utilitaire *keytool* pour importer le fichier du certificat de sécurité afin de générer un fichier de clés local :

   keytool -import -alias ALIAS -file CERTIFICATE_FILE -keystore KEYSTORE_FILE

   Exemple : **keytool -import -alias RHEVM36vmwt9 -file hjs495-vmw-t-9.cer -keystore RHEVM36KeyStore**

   Où

   ALIAS Référence unique pour chaque certificat ajouté au fichier de clés certifiées de l'agent ; par exemple, *datasource* est un alias approprié pour le certificat provenant de *datasource.example.com*.

   FICHIER_CERTIFICAT
   Nom et chemin d'accès complet au fichier de certificat de source de données en cours d'ajout au magasin de clés de confiance.

   FICHIER_CLES
   Nom du fichier de clés que vous voulez spécifier.

   Conseil : L'utilitaire *keytool* est disponible avec Java Runtime Environment (JRE). Le fichier de clés est stocké au même emplacement que celui où vous exécutez la commande.

3. Vérifiez que l'utilisateur, qui se connecte à RHEVM, est un administrateur doté du rôle SuperUser (superutilisateur). Vous pouvez utiliser un ID utilisateur existant ayant ce rôle, ou en créer un nouveau en procédant comme décrit à la section «Création d'un utilisateur et attribution des droits nécessaires», à la page 439.

Procédure

1. A partir d'une ligne de commande, exécutez la commande suivante :

   rép_install/bin/linux_kvm-agent.sh config nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config nom_instance**

   Où

   nom_instance
   Est le nom que vous voulez attribuer à l'instance.

   rép_install
   Chemin où l'agent est installé.

2. Répondez aux invites et indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration pour la connexion au serveur RHEVM», à la page 446.

3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/linux_kvm-agent.sh start nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start nom_instance**

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration d'une connexion au serveur RHEVH

Pour configurer une connexion au serveur RHEVH, vous devez exécuter le script et répondre aux invites.

Avant de commencer

- Vérifiez que l'utilisateur qui se connecte à RHEVM est un superutilisateur. Vous pouvez utiliser un ID utilisateur existant ou en créer un nouveau en procédant comme décrit à la section «Création d'un utilisateur et attribution des droits nécessaires», à la page 439.
- Configurez le protocole que vous voulez utiliser pour vous connecter au serveur RHEVH en procédant comme décrit à la section «Configuration des protocoles», à la page 440.

Procédure

1. A partir d'une ligne de commande, exécutez la commande suivante :

   rép_install/bin/linux_kvm-agent.sh config nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config nom_instance**

   Où

   nom_instance
   Est le nom que vous voulez attribuer à l'instance.

   rép_install
   Chemin où l'agent est installé.
2. Répondez aux invites et indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration pour la connexion au serveur RHEVH», à la page 448.
3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/linux_kvm-agent.sh start nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start nom_instance**

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration pour la connexion au serveur RHEVM

Vous pouvez modifier les valeurs par défaut des paramètres de configuration qui sont utilisés pour connecter l'agent avec le serveur RHEVM.

Le tableau ci-après contient une description détaillée des paramètres de configuration.

Tableau 126. Noms et descriptions des paramètres de configuration pour la connexion au serveur RHEVM

Nom du paramètre	Description	Zone obligatoire
Edit Monitoring Agent for Linux KVM settings	Indique que vous pouvez commencer à éditer les valeurs par défaut des paramètres de configuration. Entrez 1 (Yes) (valeur par défaut) pour continuer.	Oui

Tableau 126. Noms et descriptions des paramètres de configuration pour la connexion au serveur RHEVM (suite)

Nom du paramètre	Description	Zone obligatoire
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Level of Detail in Data Provider Log	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 = Off : aucun message n'est consigné. • 2 = Severe : seules les erreurs sont consignées. • 3 = Warning : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 = Info : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 = Fine : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 = Finer : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information très détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 = Finest : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Cette option risque d'affecter les performances de l'agent de surveillance de manière négative. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 = All : toutes les erreurs et tous les messages sont consignés.	Oui
Edit Hypervisor settings	Indique si vous voulez éditer les paramètres pour une connexion au serveur RHEVH. Entrez `5 (Next)` pour indiquer que vous configurez une connexion au serveur RHEVM. La valeur par défaut est `5 (Next)`.	Oui
Edit RHEVM Connection Details settings	Indique si vous voulez éditer les paramètres pour une connexion au serveur RHEVM. Entrez `1 (Add)` pour continuer. La valeur par défaut est `5 (Next)`. **Important :** Après avoir spécifié des valeurs pour tous les paramètres de configuration, vous êtes de nouveau invité à indiquer si vous voulez continuer à éditer les paramètres. Entrez `5 (Exit)`.	Oui
RHEVM ID	Le nom d'utilisateur unique que vous indiquez pour le RHEVM auquel vous vous connectez.	Oui

Tableau 126. Noms et descriptions des paramètres de configuration pour la connexion au serveur RHEVM (suite)

Nom du paramètre	Description	Zone obligatoire
Host	Nom d'hôte ou adresse IP de la source de données qui est utilisée pour la connexion au serveur RHEVM.	Oui
User	Nom d'utilisateur de la source de données disposant des privilèges appropriés pour se connecter au serveur RHEVM.	Oui
Password	Mot de passe associé au nom d'utilisateur permettant de se connecter au serveur RHEVM.	Oui
Re-type password	Mot de passe que vous avez indiqué dans la zone **Password**.	Oui
Port	Numéro de port utilisé pour la connexion au serveur RHEVM.	Oui
Domaine	Domaine auquel appartient l'utilisateur.	Oui
KeyStorePath	Nom et chemin d'accès au fichier de clés local que vous avez créé à l'aide de la commande **keytool**.	Oui

Paramètres de configuration pour la connexion au serveur RHEVH

Vous pouvez modifier les valeurs par défaut des paramètres de configuration qui sont utilisés pour connecter l'agent avec le serveur RHEVH.

Le tableau ci-après contient une description détaillée des paramètres de configuration.

Tableau 127. Noms et descriptions des paramètres de configuration pour la connexion à l'hyperviseur

Nom du paramètre	Description	Zone obligatoire
Edit Monitoring Agent for Linux KVM settings	Indique que vous pouvez commencer à éditer les valeurs par défaut des paramètres de configuration. Entrez 1 (Yes) (valeur par défaut) pour continuer.	Oui
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui

Tableau 127. Noms et descriptions des paramètres de configuration pour la connexion à l'hyperviseur (suite)

Nom du paramètre	Description	Zone obligatoire
Level of Detail in Data Provider Log	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 = Off : aucun message n'est consigné. • 2 = Severe : seules les erreurs sont consignées. • 3 = Warning : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 = Info : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 = Fine : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 = Finer : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information très détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 = Finest : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Si vous sélectionnez cette option, cela risque d'affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 = All : toutes les erreurs et tous les messages sont consignés.	Oui
Edit Hypervisor settings	Indique si vous voulez éditer les paramètres pour une connexion à l'hyperviseur. Entrez `1 (Add)`. La valeur par défaut est `5 (Next)`.	Oui
Hypervisor ID	Le nom d'utilisateur unique que vous indiquez pour le RHEVH auquel vous vous connectez.	Oui
Host	Nom d'hôte ou adresse IP de la source de données qui est utilisée pour la connexion au serveur RHEVH.	Oui
User	Nom d'utilisateur de la source de données disposant des privilèges appropriés pour se connecter au serveur RHEVM.	Oui
Remote Transport	Protocole utilisé par l'API `libvirt` locale pour se connecter aux API `libvirt` distantes. La valeur par défaut est 1. Les valeurs suivantes sont admises : • 1 = SSH • 2 = TLS • 3 = TCP (non chiffré - non recommandé dans un environnement de production)	Oui
Port	Port utilisé par le protocole de transport pour se connecter à l'API `libvirt`. La valeur par défaut est 22. **Important :** Ce port n'est nécessaire que si les ports standard ont été modifiés (22 pour SSH, 16514 pour TLS, 16509 pour TCP).	Oui

Tableau 127. Noms et descriptions des paramètres de configuration pour la connexion à l'hyperviseur (suite)

Nom du paramètre	Description	Zone obligatoire
Domaine	Domaine auquel appartient l'utilisateur.	Oui
Connection Instance Type	Indique si l'API `libvirt` locale se connecte au pilote du système doté de droits ou au pilote de session utilisateur sans droit. La valeur par défaut est 1. Les valeurs suivantes sont admises : • 1 = système • 2 = session	Oui
Edit RHEVM Connection Details settings	Indique si vous voulez éditer les paramètres pour une connexion au serveur RHEVM. Entrez `1 (Add)` pour continuer. La valeur par défaut est `5 (Next)`. **Important :** Après avoir spécifié des valeurs pour tous les paramètres de configuration, vous êtes de nouveau invité à indiquer si vous voulez continuer à éditer les paramètres. Entrez `5 (Next)`.	Oui

Configuration de la surveillance de Microsoft Active Directory

L'Monitoring Agent for Microsoft Active Directory est automatiquement configuré et démarré après l'installation.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Génération d'un rapport sur la compatibilité du produit logiciel pour l'agent Microsoft Active Directory

Pour afficher les données de tous les attributs dans le tableau de bord, procédez comme suit :

- «Exécution de l'agent Microsoft Active Directory en tant qu'administrateur»
- «Configuration des variables d'environnement local», à la page 451

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent.

Exécution de l'agent Microsoft Active Directory en tant qu'administrateur

Vous devez avoir des droits d'administrateur pour exécuter l'agent Microsoft Active Directory.

Pourquoi et quand exécuter cette tâche

Tous les ensembles de données sont disponibles pour les utilisateurs membres du groupe Administrateur. Dans cette tâche, vous créez un utilisateur, affectez des droits d'administrateur à l'utilisateur et remplacez le compte utilisateur de l'agent par cet utilisateur.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils d'administration** > **Utilisateurs et ordinateurs Active Directory**.
2. Pour développer le domaine où vous souhaitez créer l'utilisateur, cliquez sur le signe (+) en regard du nom d'un domaine.

3. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau** > **Utilisateur**.
4. Pour créer un utilisateur, ouvrez l'assistant **Nouvel objet - Utilisateur**. Par défaut, un nouvel utilisateur est membre du groupe Utilisateurs du domaine.
5. Cliquez avec le bouton droit sur le nouvel utilisateur que vous venez de créer dans le groupe Utilisateurs du domaine, puis cliquez **Propriétés**. La fenêtre des propriétés du nom d'utilisateur s'affiche. Le nom d'utilisateur est le nom du nouvel utilisateur.
6. Dans la fenêtre des propriétés du nom d'utilisateur, procédez comme suit :
   a. Cliquez sur l'onglet **Membre de**. Dans la zone **Membre de**, ajoutez le groupe Administrateurs.
   b. Cliquez sur **Appliquer**, puis sur **OK**.
7. Cliquez sur **Démarrer** > **Exécuter**, puis tapez `services.msc`.
8. Dans la fenêtre Services, procédez comme suit :
   a. Cliquez avec le bouton droit de la souris sur **Agent de surveillance pour le service Active Directory** et cliquez sur **Propriétés**.
   b. Dans la fenêtre Agent de surveillance pour les propriétés Active Directory, dans l'onglet **Connexion**, cliquez sur **Ce compte**. Entrez les données d'identification de l'utilisateur.
   c. Cliquez sur **Appliquer**, puis sur **OK**.
9. Redémarrez le service d'agent.

Configuration des variables d'environnement local

Vous devez indiquer des valeurs pour les variables d'environnement pour afficher les données de réplication Sysvol dans le tableau de bord. Vous pouvez aussi éventuellement mettre à jour la valeur d'intervalle de cache afin d'activer ou de désactiver la mise en cache.

Procédure

1. Dans la fenêtre IBM Performance Management, dans le menu **Actions**, cliquez sur **Advanced** > **Edit ENV File**.
2. Dans le fichier `K3ZENV`, changez les valeurs des variables d'environnement suivantes.

   ADO_CACHE_INTERVAL
   Détermine si la mise en cache doit être démarrée ou arrêtée et définit une valeur d'intervalle de mise en cache. L'intervalle de mise en cache est la durée en secondes entre deux collectes consécutives de données. Entrez un entier positif pour l'intervalle de mise en cache afin de démarrer la mise en cache. Entrez la valeur zéro pour l'intervalle de mise en cache afin d'arrêter la mise en cache. Par défaut, la mise en cache est démarrée et l'intervalle de mise en cache défini sur 1200.

   ADO_SYSVOL_FORCE_REPLICATION_FLAG
   Détermine si la réplication forcée qui est initiée par l'agent est activée ou désactivée. La valeur par défaut de cette variable est `TRUE`. Pour désactiver la réplication forcée, affectez à cette variable la valeur `FALSE`.

   ADO_SYSVOL_REPLICATION_TEST_INTERVAL
   Détermine l'intervalle de temps en minutes entre deux tests de réplication Sysvol. La valeur par défaut de cette variable est `0` minutes. Pour effectuer le test de réplication Sysvol, assurez-vous que la valeur de cette variable est supérieure à zéro.

   ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL
   Détermine le délai d'attente en minutes de l'agent avant de vérifier les résultats de la réplication Sysvol après avoir effectué le test de réplication Sysvol.

   La valeur de la variable **ADO_SYSVOL_REPLICATION_TEST_INTERVAL** doit être supérieure à celle de la variable **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL**. Vous pouvez utiliser les valeurs suivantes pour ces variables :

   ADO_SYSVOL_REPLICATION_TEST_INTERVAL : `1440`

ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL : 30

Une fois que des valeurs valides ont été affectées aux deux variables d'environnement, l'agent Active Directory crée un fichier dans le dossier partagé Sysvol du système géré et lance la réplication Sysvol forcée. Cette réplication forcée est démarrée du système géré vers les dossiers partagés Sysvol des partenaires de réplication Sysvol. Après vérification des résultats du test de réplication, l'agent supprime les fichiers créés et répliqués du système géré et des partenaires de réplication Sysvol.

3. Facultatif : Dans le fichier K3ZENV, ajoutez la variable d'environnement **APM_ATTRIBUTES_ENABLE_COLLECTION** et définissez sa valeur sur Yes pour visualiser des données pour les ensembles de données suivants dans l'onglet **Détails d'attribut**.
   - Services
   - Réplication
   - File Replication Service (FRS)
   - Unité d'org déplacée ou supprimée
   - LDAP
   - Gestionnaire de comptes de la sécurité
   - DFS
   - Carnet d'adresses
   - Journal des événements
   - Objets de configuration de mot de passe

   A faire : Si vous voulez désactiver la collecte de données pour ces ensembles de données, définissez la valeur pour la variable d'environnement **APM_ATTRIBUTES_ENABLE_COLLECTION** sur No.
4. Redémarrez l'agent Microsoft Active Directory.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Exécution de l'agent Microsoft Active Directory en tant qu'utilisateur non-administrateur

Vous pouvez exécuter Log File Agent en tant qu'utilisateur non-administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter l'agent de surveillance pour Active Directory en tant qu'utilisateur non-administrateur ; cependant, les attributs Topologie d'accréditation et Réplication Sysvol peuvent être indisponibles. Ces attributs ne sont disponibles que pour les utilisateurs de domaine.

Pour afficher les attributs Topologie d'accréditation, un utilisateur non-administrateur doit disposer des autorisations suivantes sur le Registre :

- Droits d'accès complets au répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Candle.
- Droits d'accès en lecture au répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Perflib.

Pour afficher les attributs Réplication Sysvol, un utilisateur non-administrateur doit disposer de droits d'accès complets au dossier Sysvol sur tous les contrôleurs de domaine d'un domaine.

Important : Lorsque vous exécutez l'agent Microsoft Active Directory en tant qu'utilisateur non-administrateur, certains services du groupe d'attributs Services indiquent que les valeurs des attributs Etat actuel et Type de démarrage sont inconnues dans l'interface utilisateur d'APM.

Le tableau suivant contient les groupes d'attributs pour l'agent Active Directory, qui affichent les données des utilisateurs de domaine et des utilisateurs de surveillance des performances.

Tableau 128. Groupes d'attributs des utilisateurs de domaine et des utilisateurs de surveillance des performances

Droits d'utilisateur	**Groupe d'attributs**
Utilisateurs de domaine	• Informations sur le pool RID • Services • Journaux des événements • DNS • Détails de l'intégration à AD DNS • Intégration à AD DNS • DHCP • Accréditation • Objets de stratégie de groupe • Objets perdus et trouvés • Service d'annuaire d'échange • Objets de conflit de réplication • Attribut LDAP • Serveur de répertoire principal • Conteneurs • Partenaire de réplication • Disponibilité du contrôleur de domaine • Temps d'attente de partenaire de réplication • Topologie de forêt

Tableau 128. Groupes d'attributs des utilisateurs de domaine et des utilisateurs de surveillance des performances (suite)

Droits d'utilisateur	Groupe d'attributs
Utilisateurs de domaine et utilisateurs de surveillance des performances	Tous les attributs répertoriés pour les utilisateurs de domaine auxquels s'ajoutent les groupes d'attributs supplémentaires suivants : • Carnet d'adresses • Réplication • Services d'annuaire • Vérificateur de cohérence des données • Centre de distribution de clés kerberos • Protocole LDAP (Lightweight Directory Access Protocol) • Autorité de sécurité locale (LSA) • Fournisseur de service d'annuaire • Gestionnaire de comptes de la sécurité • File Replication Service (FRS) • Réplication de système de fichiers réparti • Connexions de réplication DFS • Dossiers répliqués DFS • Volume de service DFS • Performances du contrôleur de domaine • Serveur d'accès distant • Serveur d'accès direct • Attributs Netlogon

Remarque : De plus, les groupes d'attributs suivants affichent les données des utilisateurs membres du groupe *Administrateurs* :

- Informations sur les bases de données Active Directory
- Unité organisationnelle déplacée ou supprimée
- Objets de configuration de mot de passe

Pour plus d'informations, voir «Configuration de la surveillance de Microsoft Active Directory», à la page 450.

Procédure

1. Cliquez sur **Démarrer>Programmes>Administrative Outils>Utilisateurs et ordinateurs Active Directory**.
2. Développez le domaine dans lequel vous voulez créer l'utilisateur en cliquant sur le signe plus (+) qui se trouve en regard de son nom.
3. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau>Utilisateur**.
4. Créez un nouvel utilisateur à l'aide de l'assistant Nouvel objet - Utilisateur. Par défaut, tout nouvel utilisateur fait partie du groupe Utilisateurs du domaine.
5. Cliquez avec le bouton droit de la souris sur le nouvel utilisateur que vous venez de créer dans le groupe *Utilisateurs du domaine*, puis cliquez sur **Propriétés**. La fenêtre Propriétés de Nom d'utilisateur s'ouvre, où *nom_utilisateur* est le nom du nouvel utilisateur. Exécutez les étapes suivantes dans la fenêtre Propriétés de Nom d'utilisateur :
   a. Cliquez sur l'onglet **Membre de**. Dans la zone Membre de, ajoutez le groupe Performance Monitor Users (Utilisateurs du moniteur de performances).

b. Cliquez sur **Appliquer**, puis sur **OK**.

6. Accédez au répertoire `rép_principal_candle`. Le chemin par défaut est `C:\IBM\APM`.
7. Cliquez avec le bouton droit de la souris sur le dossier `APM`, puis cliquez sur **Propriétés**. La fenêtre Propriétés d'APM s'affiche. Exécutez les étapes suivantes dans la fenêtre Propriétés d'APM :
   a. Sur l'onglet **Sécurité**, cliquez sur **Editer**.
   b. Cliquez sur **Ajouter** pour ajouter le nouvel utilisateur et lui accorder des droits d'accès complets.
   c. Cliquez sur **Appliquer**, puis sur **OK**.
8. Cliquez sur **Démarrer>Exécuter**, puis tapez `services.msc`. La fenêtre Services s'ouvre. Exécutez les étapes suivantes dans la fenêtre Services :
   a. Cliquez avec le bouton droit de la souris sur **Agent de surveillance** pour le service Active Directory, puis cliquez sur **Propriétés**.
   b. Dans la fenêtre Propriétés d'Active Directory, sous l'onglet **Connexion**, cliquez sur **Ce compte**. Entrez les données d'identification de l'utilisateur.
   c. Cliquez sur **Appliquer**, puis sur **OK**.
9. Redémarrez le service d'agent.

Configuration de la surveillance de Microsoft Cluster Server

Vous devez configurer l'Monitoring Agent for Microsoft Cluster Server pour qu'il puisse collecter les données du serveur en cluster. Utilisez le fichier de réponses silencieux pour configurer l'agent.

Avant de commencer

Veillez à exécuter les tâches suivantes :

- Créez un groupe de ressources vide pour l'agent.
- Créez une ressource de cluster de service générique dans le groupe de ressources de l'agent sur les systèmes Windows Server 2008 et 2012.
- Vérifiez que l'utilisateur, qui se connecte à l'environnement ou à l'application Microsoft Cluster Server, dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

  A faire : Pour configurer l'agent Microsoft Cluster Server, vous pouvez utiliser un utilisateur local ou un utilisateur de domaine à condition que celui-ci dispose des privilèges d'administrateur.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Cluster Server.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 129. Versions d'agent et documentation

Version de l'agent Microsoft Cluster Server	Documentation
06.31.10.00, 06.31.09.00	IBM Cloud Application Performance Management
06.31.09.00	IBM Performance Management 8.1.3 *
06.31.07.00	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Pourquoi et quand exécuter cette tâche

L'agent Microsoft Cluster Server est un agent à instance unique. Vous devez installer et configurer l'agent manuellement de la même manière sur chaque noeud du cluster. Pour configurer l'agent, voir «Configuration de l'agent en utilisant le fichier de réponses silencieux».

Création d'une ressource de cluster de service générique sur des systèmes Windows Server 2008 et 2012

Vous devez ajouter le service d'agent de cluster en tant que ressource pour que l'agent puisse surveiller le serveur en cluster.

Avant de commencer

Vérifiez que l'agent est arrêté sur chaque noeud du cluster.

Procédure

Pour créer une ressource de cluster de service générique, procédez comme suit :

1. Ouvrez le Gestionnaire du cluster de basculement sur l'un des noeuds du cluster.
2. Effectuez l'une des étapes suivantes :
   - Pour Windows Server 2008 :

     Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur **Services et applications**, puis cliquez sur **Plus d'actions** > **Créer un service ou une application vide**. Le nouveau service s'affiche dans la liste des services et applications.
   - Pour Windows Server 2012 :

     Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur **Rôles**, puis cliquez sur **Plus d'actions** > **Créer des rôles**. Le nouveau service s'affiche dans la liste des rôles.
3. Renommez le nouveau service créé.
4. Cliquez sur le nouveau service avec le bouton droit de la souris, puis cliquez sur **Ajouter une ressource** > **Service générique**.
5. Dans la fenêtre Assistant Nouvelle ressource, sélectionnez **Agent de surveillance pour Microsoft Cluster Server**, puis cliquez sur **Suivant**.
6. Cliquez sur **Suivant** dans les fenêtres qui suivent jusqu'à afficher le bouton **Terminer**.
7. Cliquez sur **Terminer**. Le service d'agent est ajouté en tant que ressource.
8. Cliquez avec le bouton droit de la souris sur la ressource **Agent de surveillance pour Microsoft Cluster Server**, puis cliquez sur **Mettre la ressource en ligne**.

Résultats

L'agent est démarré sur le noeud préférentiel.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent Microsoft Cluster Server dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour définir des valeurs différentes pour les paramètres de configuration.

Avant de commencer

Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent à l'aide du fichier de réponses silencieux.

Procédure

1. Ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*\samples\microsoft_cluster_server_silent_config.txt
2. Pour la variable d'environnement **CTIRA_HOSTNAME**, indiquez le nom de cluster sous forme de valeur.
3. Sur chaque noeud du cluster, exécutez la commande suivante : **rép_install\BIN\microsoft_cluster_server-agent.bat config rép_install\samples\microsoft_cluster_server_silent_config.txt**

Que faire ensuite

Modifiez le compte utilisateur d'utilisateur local à utilisateur de domaine.

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft Cluster Server, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche

Par défaut, l'agent s'exécute avec le compte utilisateur local. Il doit s'exécuter avec l'utilisateur de domaine pour pouvoir surveiller tous les noeuds du cluster à partir d'un seul noeud.

Procédure

Pour modifier le compte utilisateur, procédez comme suit :

1. Ouvrez la fenêtre IBM Performance Management.
2. Cliquez sur l'agent avec le bouton droit de la souris, puis cliquez sur **Modifier le démarrage**.
3. Entrez les données d'identification de connexion du domaine.
4. Ouvrez le Gestionnaire du cluster de basculement sur l'un des noeuds et démarrez le service de cluster.

Résultats

L'agent est démarré sur le noeud.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Performance Management, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de la surveillance de Microsoft Exchange

Vous devez configurer Monitoring Agent for Microsoft Exchange Server pour surveiller la disponibilité et les performances des serveurs Exchange.

Avant de commencer

Pour pouvoir configurer l'agent, veillez à exécuter les tâches suivantes :

- «Création d'utilisateurs», à la page 458

- «Affectation des droits d'administrateur à l'utilisateur de Serveur Exchange», à la page 461
- «Attribution à l'utilisateur de Serveur Exchange des droits d'administrateur local», à la page 463
- «Configuration du Serveur Exchange pour l'accessibilité», à la page 465
- «Configuration de l'agent pour qu'il s'exécute sous l'utilisateur de domaine», à la page 466
- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Exchange Server.

Pourquoi et quand exécuter cette tâche

Vous pouvez démarrer l'agent Microsoft Exchange Server une fois installé. Une configuration manuelle est toutefois requise pour afficher les données pour tous les attributs d'agent.

- Pour configurer l'agent en local, voir «Configuration de l'agent en local», à la page 466.
- Pour configurer l'agent en utilisant le fichier de réponses silencieux, voir «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 470.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour les versions antérieures de l'agent, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management :

- 6.3.1.11
- 6.3.1.10
- 6.3.1.9

Création d'utilisateurs

Vous pouvez créer un utilisateur pour l'agent sur le serveur Exchange manuellement ou en exécutant l'utilitaire *Nouvel utilisateur*. Vous devez créer l'utilisateur sur chaque Serveur Exchange à surveiller.

Avant de commencer

Installez l'agent Microsoft Exchange Server. Pour créer un utilisateur, vous devez être un administrateur de domaine ayant des droits d'administration complets sur Microsoft Exchange Server.

Pourquoi et quand exécuter cette tâche

Utilisez l'une des procédures suivantes pour créer des utilisateurs :

- «Création d'utilisateur sur Exchange Server 2007 et 2010»
- «Création d'utilisateur sur Exchange Server 2013», à la page 460
- «Création d'utilisateurs à l'aide de l'utilitaire Nouvel utilisateur», à la page 460

Création d'utilisateur sur Exchange Server 2007 et 2010

Vous devez créer un utilisateur pour l'agent sur Exchange Server 2007 et 2010 afin que l'agent puisse communiquer et s'authentifier avec le Serveur Exchange à surveiller.

Procédure

Pour créer un utilisateur, procédez comme suit :

1. Cliquez sur **Démarrer > Tous les programmes > Microsoft Exchange Server 2007 > Exchange Management Console**. La fenêtre Exchange Management Console s'ouvre.
2. Dans l'arborescence de la console, cliquez sur **Boîte aux lettres dans la Configuration du destinataire**.
3. Dans le panneau Action, cliquez sur **Nouvelle boîte aux lettres**. L'assistant Nouvelle boîte aux lettres s'ouvre.

4. Dans la page Introduction, cliquez sur **Boîte aux lettres de l'utilisateur**.
5. Dans la page Type d'utilisateur, cliquez sur **Nouvel utilisateur**.
6. Dans la page Informations utilisateur, renseignez les zones suivantes :

   Unité organisationnelle
   Par défaut, le conteneur Utilisateurs d'Active Directory s'affiche. Cliquez sur **Parcourir** pour modifier l'unité organisationnelle par défaut.

   Prénom
   Entrez le prénom de l'utilisateur.

   Second prénom
   Entrez les initiales de l'utilisateur.

   Nom Entrez le nom de l'utilisateur.

   Nom Par défaut, le prénom, les initiales et le nom de famille sont affichées dans cette zone. Vous pouvez modifier le nom.

   Nom de connexion de l'utilisateur (Nom principal de l'utilisateur)
   Entrez le nom que l'utilisateur devra saisir pour se connecter à la boîte aux lettres.

   Nom de connexion de l'utilisateur (versions antérieures à Windows 2000)
   Entrez le nom d'utilisateur compatible avec Microsoft Windows 2000 Server ou version antérieure.

   Mot de passe
   Entrez le mot de passe que l'utilisateur devra saisir pour se connecter à la boîte aux lettres.

   Confirmer le mot de passe
   Entrez le mot de passe que vous avez entré dans la zone **Mot de passe** une seconde fois.

   L'utilisateur doit changer de mot de passe à la prochaine connexion
   Cochez cette case si vous souhaitez que l'utilisateur réinitialise le mot de passe.
7. Dans la page Paramètres de la boîte aux lettres, renseignez les zones suivantes :

   Alias Par défaut, la valeur de cette zone est identique à celle que vous avez spécifiée dans la zone **Nom de connexion de l'utilisateur (Nom principal de l'utilisateur)**.

   Base de données de la boîte aux lettres
   Cliquez sur **Parcourir** pour ouvrir la fenêtre Sélectionnez la base de données de boîtes aux lettres. Sélectionnez la base de données que vous souhaitez utiliser, puis cliquez sur **OK**.

   Stratégie de boîte aux lettres de dossier géré
   Cochez cette case pour définir une stratégie de gestion des enregistrements de messagerie (MRM). Cliquez sur **Parcourir** pour sélectionner la stratégie de boîtes aux lettres de dossier géré à associer à cette boîte aux lettres.

   Stratégie de boîte aux lettres Exchange ActiveSync
   Cochez cette case pour définir une stratégie de boîte aux lettres Exchange ActiveSync. Cliquez sur **Parcourir** pour sélectionner la stratégie de boîtes aux lettres Exchange ActiveSync à associer à cette boîte aux lettres.
8. Sur la page Nouvelle boîte aux lettres, vérifiez le récapitulatif de configuration. Cliquez sur **Nouveau** pour créer une boîte aux lettres. Dans la page d'achèvement, la section de résumé indique si la boîte aux lettres a été créée.
9. Cliquez sur **Terminer**.

Que faire ensuite

Attribuez des droits d'administrateur à l'utilisateur Exchange que vous avez créé.

Création d'utilisateur sur Exchange Server 2013

Vous devez créer un utilisateur pour l'agent sur Exchange Server 2013 afin que l'agent puisse communiquer et s'authentifier avec le Serveur Exchange à surveiller.

Procédure

Pour créer un utilisateur sous Exchange Server 2013, procédez comme suit :

1. Connectez-vous au centre d'administration Exchange à l'aide de vos informations d'identification.
2. Dans Centre d'administration Exchange, cliquez sur **destinataires** dans le coin supérieur gauche de la page, puis cliquez sur **boîtes aux lettres**.
3. Cliquez sur la flèche vers le bas en regard du signe (+) qui se trouve sous l'option **boîtes aux lettres**, puis cliquez sur **Boîte aux lettres de l'utilisateur**.
4. Dans la page «Nouvelle boîte aux lettres de l'utilisateur», cliquez sur **Nouvel utilisateur**, puis indiquez des valeurs pour les autres zones.
5. Cliquez sur **Sauvegarder**.

Que faire ensuite

Attribuez des droits d'administrateur à l'utilisateur Exchange que vous avez créé.

Création d'utilisateurs à l'aide de l'utilitaire Nouvel utilisateur

Vous pouvez exécuter l'utilitaire Nouvel utilisateur pour créer des utilisateurs sous Exchange Server 2007 ou version ultérieure. L'utilisateur créé à l'aide de cet utilitaire dispose de toutes les autorisations requises pour exécuter l'agent. Cet utilitaire s'installe en même temps que l'agent.

Avant de commencer

Vérifiez que l'agent est installé. Pour exécuter l'utilitaire Nouvel utilisateur, vous devez être un administrateur de domaine doté de tous les droits d'administrateur sur Microsoft Exchange Server.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez cet utilitaire, l'utilisateur est créé dans le groupe Users d'Active Directory et dispose des droits suivants :

- Sous Exchange Server 2007 :
  - Administrateur local
  - Utilisateur du bureau à distance
  - Administrateur des destinataires Exchange
- Sous Exchange Server 2010, ou version ultérieure :
  - Administrateur local
  - Utilisateur du bureau à distance
  - Serveurs Exchange ou Gestion des dossiers publics.

Procédure

Pour exécuter l'utilitaire Nouvel utilisateur, procédez comme suit :

1. Cliquez deux fois sur le fichier `kexnewuser.exe` qui est disponible à l'emplacement suivant : *`rép_install`*`\TMAITM6_x64`, où *rép_install* correspond au chemin où l'agent est installé.
2. Dans la fenêtre Nouvel utilisateur, procédez comme suit :
   a. Entrez le prénom et le nom de l'utilisateur.

      Restriction : La longueur du prénom et du nom ne doit pas dépasser 28 caractères.

b. Dans la zone **Nom de connexion de l'utilisateur**, entrez le nom que l'utilisateur doit taper lors de la connexion.

   Restriction : La longueur du nom de connexion de l'utilisateur ne doit pas dépasser 256 caractères.

c. Dans la zone **Mot de passe**, entrez votre mot de passe.

d. Dans la zone **Confirmez le mot de passe**, entrez à nouveau votre mot de passe.

e. Sélectionnez **L'utilisateur doit changer de mot de passe à la prochaine connexion** si vous souhaitez que le mot de passe indiqué soit réinitialisé lors de la prochaine connexion de l'utilisateur.

f. Cliquez sur **Suivant**.

Les valeurs de configuration que vous spécifiez sont validées et des messages d'erreur s'affichent en cas de valeurs incorrectes.

3. Dans la liste des bases de données de la boîte aux lettres, sélectionnez la base de données de la boîte aux lettres requise, puis cliquez sur **Suivant**. Un récapitulatif des valeurs de configuration s'affiche.
4. Cliquez sur **Terminer**.

Résultats

Les paramètres sont sauvegardés et l'utilisateur est créé.

Affectation des droits d'administrateur à l'utilisateur de Serveur Exchange

L'utilisateur que vous avez créé pour l'agent Microsoft Exchange Server doit être un administrateur de domaine disposant de tous les droits d'administrateur sous Microsoft Exchange Server. Les droits d'administrateur sont nécessaires pour pouvoir accéder aux composants agent Microsoft Exchange Server.

Avant de commencer

Créez un utilisateur de Serveur Exchange dont la boîte aux lettres se trouve sur le Serveur Exchange qui est surveillé.

Pourquoi et quand exécuter cette tâche

Utilisez l'une des procédures ci-dessous pour affecter des droits administrateur à l'utilisateur :

- «Affectation des droits d'administrateur sous Exchange Server 2007»
- «Affectation des droits d'administrateur sous Exchange Server 2010», à la page 462
- «Affectation des droits d'administrateur sous Exchange Server 2013», à la page 462
- «Affectation des droits d'administrateur sous Exchange Server 2016», à la page 462

Affectation des droits d'administrateur sous Exchange Server 2007

Sous Exchange Server 2007, vous devez affecter à l'utilisateur des droits d'Administrateur des destinataires Exchange.

Procédure

1. Cliquez sur **Démarrer > Tous les programmes > Microsoft Exchange Server 2007 > Exchange Management Console**. La fenêtre Exchange Management Console s'ouvre.
2. Dans l'arborescence de la console, cliquez sur **Configuration de l'organisation**.
3. Dans le panneau Action, cliquez sur **Ajouter un administrateur Exchange**.
4. Sur la page Ajouter un administrateur Exchange, cliquez sur **Parcourir**. Sélectionnez le nouvel utilisateur que vous avez créé, puis sélectionnez le rôle **Administrateur des destinataires Exchange**.

5. Cliquez sur **Ajouter**.
6. Sur la page Achèvement, cliquez sur **Terminer**.

Affectation des droits d'administrateur sous Exchange Server 2010

Sous Exchange Server 2010, vous devez affecter à l'utilisateur le droit Serveurs Exchange ou Gestion des dossiers publics.

Procédure

1. Connectez-vous au serveur Exchange avec des privilèges d'administrateur.
2. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur.**
3. Dans le panneau de gauche, développez **Outils**.
4. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
5. Développez **Domaine**, puis cliquez sur **Groupes de sécurité Microsoft Exchange Security**.
6. Cliquez avec le bouton droit sur **Serveurs Exchange ou Gestion des dossiers publics**, puis cliquez sur **Propriétés**.
7. Dans la fenêtre Propriétés des serveurs Exchange ou Propriétés de la gestion des dossiers publics, accédez à **Membres** et cliquez sur **Ajouter**.
8. De la liste des utilisateurs, sélectionnez l'utilisateur que vous voulez ajouter au groupe, puis cliquez sur **OK**.
9. Cliquez sur **OK**.

Affectation des droits d'administrateur sous Exchange Server 2013

Sous Exchange Server 2013, vous devez affecter à l'utilisateur le droit Serveurs Exchange ou Gestion des dossiers publics.

Procédure

1. Connectez-vous au serveur Exchange avec des privilèges d'administrateur.
2. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur.**
3. Dans le panneau de gauche, développez **Outils**.
4. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
5. Développez **Domaine**, puis cliquez sur **Groupes de sécurité Microsoft Exchange Security**.
6. Cliquez avec le bouton droit sur **Serveurs Exchange ou Gestion des dossiers publics**, puis cliquez sur **Propriétés**.
7. Dans la fenêtre Propriétés des serveurs Exchange ou Propriétés de la gestion des dossiers publics, accédez à **Membres** et cliquez sur **Ajouter**.
8. De la liste des utilisateurs, sélectionnez l'utilisateur que vous voulez ajouter au groupe, puis cliquez sur **OK**.
9. Cliquez sur **OK**.

Affectation des droits d'administrateur sous Exchange Server 2016

Sous Exchange Server 2016, vous devez affecter à l'utilisateur le droit Serveurs Exchange ou Gestion des dossiers publics.

Procédure

1. Connectez-vous au serveur Exchange avec des privilèges d'administrateur.
2. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur.**
3. Dans le panneau de gauche, développez **Outils**.
4. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
5. Développez **Domaine**, puis cliquez sur **Groupes de sécurité Microsoft Exchange Security**.

6. Cliquez avec le bouton droit sur **Serveurs Exchange ou Gestion des dossiers publics**, puis cliquez sur **Propriétés**.
7. Dans la fenêtre Propriétés des serveurs Exchange ou Propriétés de la gestion des dossiers publics, accédez à **Membres** et cliquez sur **Ajouter**.
8. De la liste des utilisateurs, sélectionnez l'utilisateur que vous voulez ajouter au groupe, puis cliquez sur **OK**.
9. Cliquez sur **OK**.

Que faire ensuite

Attribuez à l'utilisateur des droits d'administrateur local sur l'ordinateur sur lequel est installé le Serveur Exchange.

Attribution à l'utilisateur de Serveur Exchange des droits d'administrateur local

Pour accéder aux données du Serveur Exchange, l'utilisateur que vous avez créé pour l'agent Microsoft Exchange Server doit être un administrateur local de l'ordinateur sur lequel le Serveur Exchange est installé.

Avant de commencer

Créez un utilisateur de Serveur Exchange.

Pourquoi et quand exécuter cette tâche

Utilisez l'une des procédures ci-dessous pour attribuer à l'utilisateur des droits d'administrateur local :

- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2003»
- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2008», à la page 464
- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2012», à la page 464
- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2016», à la page 464

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2003

Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows 2003 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez avec le bouton droit de la souris sur **Poste de travail** sur le bureau de l'ordinateur et sélectionnez **Gérer**.
2. Développez **Utilisateurs et groupes locaux**.
3. Cliquez sur **Groupes**.
4. Cliquez deux fois sur **Administrateurs** pour afficher la fenêtre Propriétés des administrateurs.
5. Cliquez sur **Ajouter**.
6. Sélectionnez **Tout l'annuaire** dans la liste **Rechercher dans**.
7. Sélectionnez le nom de l'utilisateur que vous avez créé et cliquez sur **Ajouter**.
8. Cliquez sur **OK**.
9. Cliquez sur **OK**.

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2008

Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows Server 2008 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur**.
2. Dans le panneau de navigation, développez **Configuration**.
3. Cliquez deux fois sur **Utilisateurs et groupes locaux**.
4. Cliquez sur **Groupes**.
5. Cliquez avec le bouton droit de la souris sur le groupe auquel vous voulez ajouter le compte utilisateur, puis cliquez sur **Ajouter au groupe**.
6. Cliquez sur **Ajouter**, puis tapez le nom du compte utilisateur.
7. Cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2012

Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows Server 2012 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez sur **Démarrer > Gestionnaire de serveur**.
2. Dans le coin supérieur droit de la page Tableau de bord du Gestionnaire de serveur, cliquez sur **Outils > Gestion de l'ordinateur**.
3. Dans le panneau de navigation de la page Gestion de l'ordinateur, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Utilisateurs**.
4. Dans la liste des utilisateurs, cliquez avec le bouton droit de la souris sur l'utilisateur auquel vous voulez attribuer des droits d'administrateur, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Appartient à**, puis sur **Ajouter**.
6. Dans la page Sélectionner un groupe, entrez `Administrateurs`, puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** et sur **OK**.

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2016

Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows Server 2016 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez sur **Démarrer > Gestionnaire de serveur**.
2. Dans le coin supérieur droit de la page Tableau de bord du Gestionnaire de serveur, cliquez sur **Outils > Gestion de l'ordinateur**.
3. Dans le panneau de navigation de la page Gestion de l'ordinateur, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Utilisateurs**.
4. Dans la liste des utilisateurs, cliquez avec le bouton droit de la souris sur l'utilisateur auquel vous voulez attribuer des droits d'administrateur, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Appartient à**, puis sur **Ajouter**.
6. Dans la page Sélectionner un groupe, entrez `Administrateurs`, puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** et sur **OK**.

Configuration du Serveur Exchange pour l'accessibilité

Pour vérifier l'accessibilité, l'agent Microsoft Exchange Server envoie un message électronique au serveur et mesure le temps nécessaire pour recevoir une réponse automatique. Avant de démarrer l'agent, vous devez configurer le Serveur Exchange pour la réponse automatique aux messages électroniques.

Avant de commencer

Avant de configurer le Serveur Exchange, vérifiez que les tâches suivantes ont été effectuées :

- Une boîte aux lettres est créée pour l'utilisateur sur le Serveur Exchange que vous souhaitez surveiller.
- L'utilisateur que vous avez créé pour l'agent est un utilisateur de domaine.
- Les serveurs de votre organisation Microsoft Exchange sont configurés pour le flux de messagerie entre les serveurs.

Procédure

Utilisez la procédure suivante pour chaque Serveur Exchange dont vous souhaitez vérifier l'accessibilité :

1. Connectez-vous à Microsoft Outlook en indiquant les données d'identification de l'utilisateur que vous avez créé.
2. Cliquez sur le bouton **Suivant** de la fenêtre Bienvenue.
3. Sélectionnez **Oui**, puis cliquez sur **Suivant**.
4. Dans la zone **Microsoft Exchange Server**, indiquez le nom du Serveur Exchange.
5. Dans la zone **Boîte aux lettres**, entrez le nom de l'utilisateur que vous avez créé.
6. Cliquez sur **Terminer**.
7. Cliquez sur **OK**.
8. Cliquez sur **Outils > Règles et alertes > Nouvelle règle**.
9. Sélectionnez **Commencer à partir d'une règle vide**.
10. Sélectionnez **Vérifier les messages à leur arrivée**, puis cliquez sur **Suivant**.
11. Sélectionnez les options suivantes :
    - **Lorsque mon nom est dans la zone A :**
    - **Qui contiennent des mots spécifiques dans l'objet ou dans le corps**
12. Sous **Etape 2** dans cette fenêtre, cliquez sur **Mots spécifiques**.
13. Dans la zone **Spécifier un mot/une expression à rechercher dans l'objet/le corps du texte**, entrez `AVAILABILITY CHECK`.
14. Cliquez sur **Ajouter**.
15. Cliquez sur **OK**, puis sur **Suivant**.
16. Sélectionnez **Faire répondre le serveur avec un message spécifique** et cliquez sur **un message spécifique**.
17. Dans l'éditeur de message électronique, entrez le texte suivant dans la zone d'objet du message : `CHECK RECEIVED: MAILBOX AVAILABLE.`
18. Fermez l'éditeur de message électronique et cliquez sur **Oui** pour sauvegarder ces modifications.
19. Cliquez sur **Suivant**.
20. Lorsque vous êtes invité à définir des exceptions éventuelles, n'indiquez aucune restriction.
21. Cliquez sur **Suivant**.
22. Cliquez sur **Terminer**, puis sur **OK**.

Que faire ensuite

Configurez l'agent Microsoft Exchange Server.

Configuration de l'agent pour qu'il s'exécute sous l'utilisateur de domaine

Par défaut, l'agent Microsoft Exchange Server est configuré pour s'exécuter sous le compte de l'utilisateur local mais il doit s'exécuter sous le compte de l'utilisateur de domaine que vous avez créé.

Avant de commencer

Assurez-vous que :

- L'utilisateur que vous avez créé est un utilisateur de domaine qui dispose des droits d'administrateur local.
- L'utilisateur dispose de droits d'administrateur sur le serveur où l'agent est installé.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent s'exécute sous l'utilisateur de domaine, il peut surveiller tous les composants du Serveur Exchange.

Procédure

Pour modifier l'utilisateur sous lequel l'agent s'exécute, effectuez les étapes suivantes :

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent.
   rêp_install\InstallITM\KinCinfo.exe –r
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre Manage Monitoring Services.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme : `<Domaine\ID_Utilisateur>`, puis spécifiez le mot de passe.
6. Démarrez l'agent de surveillance.

Configuration de l'agent en local

Vous pouvez configurer l'agent en local dans la fenêtre IBM Cloud Application Performance Management.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour Microsoft Exchange Server**, puis cliquez sur **Configuration de l'agent**.

   Avertissement : Cliquez sur **Reconfigurer** si **Configuration de l'agent** est désactivé.
3. Dans la fenêtre Agent de surveillance pour Microsoft Exchange Server: Configuration avancée de l'agent, cliquez sur **OK**.
4. Dans la fenêtre Configuration d'agent, procédez comme suit :
   a. Cliquez sur l'onglet **Propriétés Exchange Server**, puis indiquez des valeurs pour les paramètres de configuration. Lorsque vous cliquez sur **OK**, les valeurs spécifiées sont validées.
   b. Cliquez sur l'onglet **Surveillance des services Exchange**, puis indiquez des valeurs pour les paramètres de configuration. Lorsque vous cliquez sur **OK**, les valeurs spécifiées sont validées.
   c. Cliquez sur l'onglet **Propriétés de configuration avancées**, puis indiquez des valeurs pour les paramètres de configuration. Lorsque vous cliquez sur **OK**, les valeurs spécifiées sont validées.

Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Configuration d'agent, consultez les rubriques suivantes :

- «Paramètres de configuration des propriétés du serveur Exchange»
- «Paramètres de configuration des services Exchange», à la page 468
- «Paramètres de configuration de l'accessibilité», à la page 469

Pour plus d'informations sur la validation des valeurs de configuration, voir «Validation des valeurs de configuration», à la page 470.

5. Recyclez l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Restriction : Dans le tableau de bord Cloud APM, les instances de l'un des types de composant Exchange uniquement (Microsoft Exchange Server ou Microsoft Exchange Server 2013) s'affichent sous Mes composants.

Paramètres de configuration des propriétés du serveur Exchange

Dans l'onglet **Propriétés Exchange Server** de la fenêtre Configuration d'agent, vous pouvez configurer les propriétés du serveur Exchange, comme le nom de serveur, le nom de domaine et le nom d'utilisateur.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'onglet **Propriétés Exchange Server**.

Tableau 130. Noms et descriptions des paramètres de configuration de l'onglet Propriétés Exchange Server.

Nom de paramètre	Description	Zone obligatoire	Exemples
Nom du serveur Exchange	Nom du Serveur Exchange. Pendant l'installation du serveur Exchange, le nom par défaut du serveur Exchange est le nom d'hôte du serveur Windows. Si vous modifiez le nom par défaut, vous devez alors utiliser le nouveau nom lors de la configuration de l'agent Exchange Server. **A faire :** Dans les environnements répartis ou en cluster, indiquez le nom du serveur de boîtes aux lettres pour Exchange Server 2007.	Oui **Important :** N'indiquez aucune valeur si l'agent est installé sur un serveur disposant d'un cluster à copie unique doté de plus de deux noeuds.	Si le nom du serveur Exchange est `popcorn`, entrez `popcorn` dans la zone **Nom du serveur Exchange**.
Nom du domaine Exchange	Nom du domaine où le Serveur Exchange est installé.	Oui	Si le serveur Exchange se trouve dans le domaine `LAB.XYZ.com`, entrez le nom qui précède le premier point, `LAB` par exemple.
Nom d'utilisateur Exchange	Nom de l'utilisateur qui est configuré pour accéder au Serveur Exchange. **A faire :** L'utilisateur doit avoir une boîte aux lettres sur le même serveur Exchange.	Oui	

Tableau 130. Noms et descriptions des paramètres de configuration de l'onglet Propriétés Exchange Server (suite).

Nom de paramètre	Description	Zone obligatoire	Exemples
Mot de passe de l'utilisateur Exchange	Mot de passe de l'utilisateur qui est configuré pour accéder au Serveur Exchange.	Oui	
Confirmer le mot de passe	Même mot de passe que celui indiqué pour l'utilisateur du serveur Exchange.	Oui	
Nom de profil MAPI Exchange	Les profils MAPI sont les paramètres de configuration principaux requis pour l'accès au serveur Exchange. Cette zone est désactivée si vous utilisez un agent Microsoft Exchange Server 64 bits pour surveiller le Serveur Exchange 2007 ou version ultérieure.	Non	
Configuration en cluster	Cochez cette case pour configurer le agent Microsoft Exchange Server dans un environnement cluster.	Sans objet	
Nom du serveur en cluster	Nom du serveur en cluster. Cette zone est activée lorsque vous sélectionnez la case à cocher **Configuration en cluster**.	Oui, si la zone est activée.	`SCCCluster`
ID du sous-système Exchange	Nom du noeud de serveur en cluster. Cette zone est activée lorsque vous sélectionnez la case à cocher **Configuration en cluster**.	Oui, si la zone est activée.	`node1`
Répertoire de données historiques de l'agent Exchange	Emplacement sur le disque où sont stockées les données d'historique. Cette zone est activée lorsque vous sélectionnez la case à cocher **Configuration en cluster**.	Oui, si la zone est activée.	`c:\history`

Paramètres de configuration des services Exchange

Dans l'onglet **Surveillance des services Exchange** de la fenêtre Configuration d'agent, vous pouvez sélectionner les services Exchange pour connaître l'état du serveur Exchange.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'onglet **Surveillance des services Exchange**.

Tableau 131. Noms et descriptions des paramètres de configuration de l'onglet Surveillance des services Exchange

Nom de paramètre	Description	Zone obligatoire
Services Exchange	Sélectionnez les services Exchange dans la liste des services disponibles et cliquez sur la flèche pour déplacer les services sélectionnés vers la liste **Services Configured for Server Status** de sorte que l'agent Microsoft Exchange Server puisse les surveiller. **A faire :** La liste des services disponibles change en fonction de la version du serveur Exchange et des rôles installés.	Sans objet
Services configurés pour le statut du serveur	Les services déjà disponibles dans cette liste déterminent le statut du Serveur Exchange. Ces services sont obligatoires et ne peuvent pas être déplacés de la liste **Services Configured for Server Status** vers la liste **Services Exchange**. Vous pouvez ajouter des services à la liste **Services Configured for Server Status** en déplaçant les services depuis la liste **Services Exchange**. Vous pouvez également redéplacer ces services supplémentaires vers la liste **Services Exchange**.	Sans objet

Paramètres de configuration de l'accessibilité

Dans l'onglet **Advanced Configuration Properties** de la fenêtre Configuration d'agent, vous pouvez configurer les paramètres liés à l'accessibilité, comme l'adresse électronique cible et l'intervalle d'accessibilité.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'onglet **Propriétés de configuration avancée**.

Tableau 132. Noms et descriptions des paramètres de configuration de l'onglet Propriétés de configuration avancées

Nom de paramètre	Description	Zone obligatoire
Activer la surveillance de l'accessibilité de la boîte aux lettres	Sélectionnez cette case à cocher si vous souhaitez que l'agent capture les données de mesure de l'accessibilité.	Sans objet
Adresse électronique cible	Adresse électronique permettant de vérifier l'accessibilité. Séparez les adresses électroniques par des points-virgules (;). **Restriction :** Le nombre total de caractères dans cette zone ne doit pas dépasser 1023.	Oui, si cette zone est activée.
Intervalle de transmission des courriers électroniques (en secondes)	Délai d'attente (en secondes) de l'agent Exchange Server entre l'envoi de courriers électroniques.	Oui, si cette zone est activée.
Délai d'attente de transmission des courriers électroniques (secondes)	Intervalle (en secondes) pendant lequel l'agent attend une réponse au courrier électronique envoyé pour tester si le serveur de boîte aux lettres est accessible.	Non
Activer la surveillance des détails de la boîte aux lettres	Sélectionnez cette case à cocher si vous souhaitez collecter des données pour les mesures détaillées de la boîte aux lettres.	Sans objet
Heure de début de la collecte des détails de la boîte aux lettres	Heure (au format hh:mm:ss) à laquelle les indicateurs de détails de la boîte aux lettres sont collectés.	Non
Intervalle de collecte des détails de la boîte aux lettres (en secondes)	Intervalle (en secondes) entre les collectes des indicateurs de détails de la boîte aux lettres.	Non
Durée de collecte des journaux d'événements (en minutes)	Durée (en minutes) pendant laquelle l'agent collecte des enregistrements d'événements.	Non
Nombre maximal d'événements	Nombre maximal d'enregistrements d'événements à collecter. La collecte des enregistrements d'événements s'arrête lorsque le nombre d'enregistrements d'événements collectés dépasse le nombre maximal.	Non
Intervalle de collecte (en secondes)	Intervalle (en secondes) entre les cycles de l'agent.	Non
Intervalle de topologie Exchange (en secondes)	Intervalle (en secondes) entre les collectes des informations détaillées sur la topologie.	Non

Tableau 132. Noms et descriptions des paramètres de configuration de l'onglet Propriétés de configuration avancées (suite)

Nom de paramètre	Description	Zone obligatoire
Intervalle de collecte de suivi des messages (heures)	Intervalle (en heures) de collecte des journaux de suivi des messages. **Restriction :** La valeur d'intervalle doit être comprise entre 1 et 12. Si vous indiquez une valeur d'intervalle supérieure à 12, la valeur enregistrée sera 12. Si vous entrez une valeur non valide qui contient des caractères alphabétiques ou des caractères spéciaux, la valeur est sauvegardée comme étant 0, ce qui signifie que la collecte de suivi des messages est désactivée. Cette zone est désactivée si l'une des conditions suivantes est vraie : • Le rôle Mailbox Server ou Hub Transport n'est pas installé sur le serveur Exchange. • La fonction de suivi de messages est désactivée sur le Serveur Exchange.	Non

Validation des valeurs de configuration

Les valeurs que vous indiquez lors de la configuration de l'agent sont validées. La validation consiste à vérifier que les valeurs sont spécifiées pour tous les paramètres obligatoires et que certaines conditions sont remplies, comme les droits d'administrateur local de l'utilisateur.

Le tableau ci-après indique les tests de validation appliqués aux valeurs de configuration spécifiées.

Tableau 133. Tests de validation

Test de validation	Vérifie si
Nom du serveur Exchange	Le nom du serveur de boîte aux lettres de l'utilisateur correspond au nom Serveur Exchange indiqué.
Droits du serveur Exchange	L'utilisateur dispose des droits requis du Serveur Exchange. Sur le Serveur Exchange 2007, l'utilisateur doit avoir les droits d'administrateur de destinataire et sur Serveur Exchange 2010, ou version ultérieure, l'utilisateur doit avoir des droits de gestion de destinataire.
Administrateur local	L'utilisateur dispose de droits d'administrateur local.
Connexion au service d'agent	Le service d'agent est configuré pour s'exécuter avec le compte utilisateur indiqué.

En cas d'échec d'un ou plusieurs tests de validation, un message d'erreur est généré. Vous devez spécifier des valeurs pour tous les paramètres obligatoires faute de quoi vous ne pourrez pas sauvegarder les valeurs configurées.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour définir des valeurs différentes pour les paramètres de configuration.

Pourquoi et quand exécuter cette tâche

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Ouvrez le fichier `msex_silent_config.txt` situé dans *`rép_install`*`\samples` et spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

2. Exécutez la commande suivante : **rép_install\BIN\msexch-agent.bat config rép_install\samples\msex_silent_config.txt**

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Restriction : Dans le tableau de bord Cloud APM, les instances de l'un des types de composant Exchange uniquement (Microsoft Exchange Server ou Microsoft Exchange Server 2013) s'affichent sous Mes composants.

Configuration des variables de l'environnement local pour l'agent

Vous pouvez configurer les variables de l'environnement local pour l'agent Microsoft Exchange Server afin d'activer ou de désactiver la régulation d'événement pour les événements en double.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, dans le menu **Actions**, cliquez sur **Advanced** > **Edit ENV File**.
3. Dans le fichier `KEXENV`, modifiez les valeurs des variables d'environnement suivantes :

   EX_EVENT_THROTTLE_ENABLE
   Cette variable vous permet de réguler les événements en double. La valeur par défaut est `False`. Pour activer la régulation d'événement afin d'éviter l'apparition d'événements en double, affectez à cette variable la valeur True.

   EX_EVENT_THROTTLE_DURATION
   Cette variable indique la durée (en minutes) de la régulation d'événement. La valeur par défaut est `0` minutes.

Configuration de la surveillance de Microsoft Hyper-V

Lorsque vous installez l'Monitoring Agent for Microsoft Hyper-V Server, il est configuré et démarré automatiquement avec les paramètres de configuration par défaut. Utilisez le fichier de réponses silencieux pour modifier les paramètres de configuration par défaut.

Avant de commencer

Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pour afficher les données de machine virtuelle sur la page de la machine virtuelle, assurez-vous d'avoir installé le composant d'intégration et l'agent de système d'exploitation sur chaque machine virtuelle. Pour les machines virtuelles exécutées sur le système Linux, veillez à exécuter les tâches suivantes :

- Mettez à niveau le système Linux.
- Installez le package `hypervkvpd` ou `hyperv-daemons rpm` mis à jour sur la machine virtuelle.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Important : Pour l'édition 8.1.3 de Performance Management, la fenêtre de configuration d'agent est supprimée car elle n'est pas requise. La fenêtre de configuration d'agent est disponible pour la version 8.1.2 ou antérieure de Performance Management.

Procédure

Pour configurer l'agent, procédez comme suit :

1. Ouvrez le fichier `microsoft_hyper-v_server_silent_config.txt` situé dans *rép_install*`\samples` et spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.
2. Ouvrez l'invite de commande et entrez la commande suivante : **rép_install\BIN\microsoft_hyper-v_server-agent.bat config rép_install\samples\microsoft_hyper-v_server_silent_config.txt**

   Le fichier de réponses contient les paramètres suivants :
   - KHV_DIRECTOR_PORT
   - KHV_DIRECTOR_SERVER

   A faire : La configuration d'agent est organisée par groupes :

   Configuration d'IBM Systems Director (IBM_DIRECTOR_CONFIGURATION)
   Les éléments de configuration définis dans ce groupe sont toujours présents dans la configuration de l'agent. Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

   Numéro de port d'IBM Systems Director Server (KHV_DIRECTOR_PORT)
   Numéro de port d'IBM Systems Director Server. La valeur par défaut est aucun.

   Nom d'hôte d'IBM Systems Director Server (KHV_DIRECTOR_SERVER)
   Nom d'hôte ou adresse IP du serveur IBM Systems Director Server qui gère l'environnement. La valeur par défaut est aucun.
3. Démarrez l'agent s'il est à l'état arrêté.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Saisie de la stratégie de sécurité locale pour l'exécution de l'Agent de surveillance pour Microsoft Hyper-V Server sous Windows par un utilisateur non-administrateur

Des stratégies de sécurité locales sont disponibles pour permettre à un utilisateur non-administrateur d'exécuter l'Monitoring Agent for Microsoft Hyper-V Server sous Windows.

Pourquoi et quand exécuter cette tâche

La combinaison des deux stratégies de sécurité locales suivantes permet à un utilisateur non-administrateur d'exécuter l'agent Microsoft Hyper-V Server sous Windows. Utilisez les deux stratégies suivantes permettant à l'agent Microsoft Hyper-V Server de démarrer/arrêter, configurer et vérifier les données.

- Déboguer les programmes
- Ouvrir une session en tant que service

Les groupes d'attributs suivants doivent également disposer de droits d'administrateur pour obtenir les données sur le portail APM :

- Disponibilité

- Migration
- Migration de la machine virtuelle sans le cluster
- Migration du stockage de la machine virtuelle

Procédez comme suit pour accorder les droits de sécurité locale à un utilisateur non-administrateur.

Procédure

1. Installez l'agent Microsoft Hyper-V Server en tant qu'administrateur local.
2. Ajoutez l'utilisateur non-administrateur dans le répertoire `rép_install` et accordez-lui les droits suivants :
   a. Accordez un accès complet au registre `HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring`.
   b. Accordez un accès en lecture au registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib` pour l'utilisateur non-administrateur.
   c. Accordez un accès complet au répertoire `rép_install` pour l'utilisateur non-administrateur.
3. Accédez au menu **Démarrer** et exécutez la commande **`secpol.msc`** pour ouvrir les stratégies de sécurité locale.
4. Pour ajouter un utilisateur non-administrateur aux stratégies, voir «Octroi de droits de la stratégie de sécurité locale».
5. Pour ajouter un utilisateur non-administrateur au groupe d'utilisateurs administrateurs Hyper-V, voir «Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V», à la page 475.
6. Pour ajouter un utilisateur non-administrateur au groupe d'utilisateurs Analyseur de performances, voir «Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs Analyseur de performances», à la page 475.
7. Pour modifier le droit de sécurité DCOM pour un utilisateur non-administrateur, voir «Modification des droits DCOM», à la page 474.
8. Redémarrez l'agent Microsoft Hyper-V Server et vérifiez les données sur le portail APM.

Octroi de droits de la stratégie de sécurité locale

Pour démarrer/arrêter, configurer et vérifier les données de l'agent Microsoft Hyper-V Server, vous devez octroyer des droits d'accès aux deux stratégies de sécurité locales suivantes : Déboguer les programmes et Ouvrir une session en tant que service.

Octroi du droit Déboguer les programmes

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, suivez la procédure relative à l'agent Microsoft Hyper-V Server décrite ci-dessous.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans la sous-fenêtre de gauche, développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des stratégies s'affiche dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre Propriétés de Déboguer les programmes apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Octroi du droit Ouvrir une session en tant que service
Pourquoi et quand exécuter cette tâche

Pour accorder le droit Ouvrir une session en tant que service, suivez la procédure relative à l'agent Microsoft Hyper-V Server décrite ci-dessous.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans la sous-fenêtre de gauche, développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des stratégies s'affiche dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre Propriétés de Ouvrir une session en tant que service apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Modification des droits DCOM

Vous devez modifier les droits DCOM pour pouvoir exécuter l'agent Microsoft Hyper-V Server avec un accès utilisateur non-administrateur.

Pourquoi et quand exécuter cette tâche

Pour modifier les droits DCOM, vérifiez que l'utilisateur possède les droits appropriés lui permettant de démarrer le serveur DCOM. Pour modifier les droits, procédez comme suit.

Procédure

1. A l'aide de la commande **Regedit**, accédez à la valeur de registre `HKCR\Clsid\*clsid value`.

   Remarque : La valeur CLSID s'affiche dans l'observateur d'événements. Elle porte l'ID événement 10016 lorsque vous configurez l'agent en tant qu'utilisateur non-administrateur.
2. Dans le panneau de droite, cliquez deux fois sur **Par défaut**.
3. Dans la boîte de dialogue Modification de la chaîne, copiez la chaîne Données de la valeur.
4. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Services de composants**.
5. Dans la fenêtre Services de composants, développez **Services de composants > Ordinateurs > Mon ordinateur** et cliquez deux fois sur **DCOM**.
6. Dans le panneau de droite, localisez la chaîne copiée (nom du programme), cliquez avec le bouton droit de la souris sur le nom du programme et cliquez sur **Propriétés**.
7. Dans la fenêtre Propriétés, cliquez sur l'onglet **Sécurité**.
8. Dans la zone Autorisations d'exécution et d'activation, sélectionnez **Personnaliser**, puis cliquez sur **Modifier**. La fenêtre Autorisations d'exécution et d'activation s'affiche.
9. Cliquez sur **Ajouter**, entrez un utilisateur non-administrateur dans la liste des droits, puis cliquez sur **OK**.
10. Cochez la case **Autoriser** en regard de Exécution locale et Activation locale, puis cliquez sur **OK**.

Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V

Vous devez ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V pour obtenir des données sur le portail APM.

Pourquoi et quand exécuter cette tâche

Pour ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Gestion de l'ordinateur**. La fenêtre Gestion de l'ordinateur s'ouvre.
2. Dans le panneau de gauche, accédez à **Outils système > Utilisateurs et groupes locaux > Groupes**. La liste des groupes s'affiche dans le panneau de droite.
3. Cliquez deux fois sur le groupe **Administrateurs Hyper-V**. La fenêtre Hyper-V Administrators Properties s'affiche.
4. Cliquez sur **Ajouter**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs Analyseur de performances

Vous devez ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs Analyseur de performances pour obtenir des données sur le portail APM.

Pourquoi et quand exécuter cette tâche

Pour ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs Analyseur de performances, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Gestion de l'ordinateur**. La fenêtre Gestion de l'ordinateur s'ouvre.
2. Dans le panneau de gauche, accédez à **Outils système > Utilisateurs et groupes locaux > Groupes**. La liste des groupes s'affiche dans le panneau de droite.
3. Cliquez deux fois sur le groupe **Utilisateurs de l'Analyseur de performances**. La fenêtre Performance Monitor Users Properties s'affiche.
4. Cliquez sur **Ajouter**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration de la surveillance de Microsoft IIS

Lorsque vous installez l'Monitoring Agent for Microsoft Internet Information Services, il est configuré automatiquement et démarre avec les paramètres de configuration par défaut.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft IIS.
- Vérifiez que l'utilisateur, qui se connecte à l'environnement ou à l'application Microsoft Internet Information Server, dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

  A faire : Pour configurer l'agent Microsoft IIS, vous pouvez utiliser un utilisateur local ou un utilisateur de domaine à condition que celui-ci dispose des privilèges d'administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 134. Versions d'agent et documentation

Version de l'agent Microsoft IIS	Documentation
6.3.1.10	IBM Cloud Application Performance Management
6.3.1.9	IBM Performance Management 8.1.3 *
6.3.1.7	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Pour configurer l'agent, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.

Que faire ensuite

Après avoir configuré l'agent, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour connaître les étapes de modification du compte utilisateur, voir «Modification du compte utilisateur», à la page 478.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Microsoft IIS sur des systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

L'agent Microsoft IIS fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Microsoft Internet Information Services**, puis sur **Configuration de l'agent**.
3. Dans la fenêtre Monitoring Agent for Microsoft Internet Information Services, procédez comme suit :
   a. Dans l'onglet **HTTP Error Log Configuration**, spécifiez un emplacement où sauvegarder le fichier journal et cliquez sur **Suivant**.

      Remarque : Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\WINDOWS\system32\LogFiles\HTTPERR`. L'administrateur peut modifier l'emplacement du fichier journal.
   b. Dans l'onglet **Site Log Configuration**, spécifiez un emplacement où sauvegarder le fichier journal et cliquez sur **OK**.

      Remarque : Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\inetpub\logs\LogFiles`. L'administrateur peut modifier l'emplacement du fichier journal.
4. Dans la fenêtre Restart of Agent de surveillance pour Microsoft IIS, cliquez sur **Yes**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Lorsque vous installez l'agent Microsoft IIS, il est configuré automatiquement et démarre avec les paramètres de configuration par défaut. Utilisez le fichier de réponses silencieux pour modifier les paramètres de configuration par défaut.

Avant de commencer

Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Procédure

Pour configurer l'agent Microsoft IIS, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire qui contient le fichier `msiis-agent.bat`.
2. Entrez la commande **`msiis-agent.bat config`** *chemin d'accès absolu au fichier de réponses*.

   Le fichier de réponses contient les paramètres suivants :

   KQ7_SITE_LOG_FILE
   C:\inetpub\logs\LogFiles

KQ7_HTTP_ERROR_LOG_FILE
C:\WINDOWS\system32\LogFiles\HTTPERR

A faire : La configuration de l'agent est organisée par groupes :

Configuration du journal du site (SITE_LOG)
Ce groupe contient les paramètres de configuration liés au fichier journal du site (KQ7_SITE_LOG_FILE). Un administrateur peut spécifier un emplacement où sauvegarder le fichier journal. Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\inetpub\logs\LogFiles`

Configuration du journal des erreurs HTTP (HTTP_ERROR_LOG)
Ce groupe contient les paramètres de configuration liés au fichier du journal des erreurs HTTP (KQ7_HTTP_ERROR_LOG_FILE). Un administrateur peut spécifier un emplacement où sauvegarder le fichier journal. Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\WINDOWS\system32\LogFiles\HTTPERR`.

3. Si l'agent est arrêté, démarrez-le.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft IIS, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche

Par défaut, l'agent Microsoft IIS s'exécute sous le compte utilisateur local.

Procédure

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent :
   rép_install\InstallITM\KinCinfo.exe –r
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre Manage Monitoring Services.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme <Domaine\ID_utilisateur>, puis indiquez le mot de passe.
6. Démarrez agent Microsoft IIS.

Configuration de la surveillance Skype for Business Server (anciennement Microsoft Lync Server)

Lorsque vous installez l'Monitoring Agent for Skype for Business Server (anciennement MS Lync Server), l'agent est à l'état non configuré. Pour le démarrer, vous devez le configurer.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Skype for Business Server.
- Assurez-vous que l'utilisateur que vous utilisez pour exécuter Agent Skype for Business Server est un utilisateur de domaine disposant des privilèges d'administrateur et des droits d'accès à tous les serveurs distants répertoriés dans la topologie de Lync ou Skype for Business Server. Utilisez un utilisateur de domaine disposant des privilèges d'administrateur, ou créez un nouvel utilisateur de domaine et affectez-lui des privilèges d'administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation de la version 6.3.1.9, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management.

Pour configurer l'agent, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.

Que faire ensuite

Après avoir configuré l'agent, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour connaître les étapes de modification du compte utilisateur, voir «Modification du compte utilisateur», à la page 482.

Droits et droits d'accès d'un utilisateur non-administrateur

Vous pouvez exécuter l'agent de surveillance pour l'Agent Skype for Business Server en tant qu'utilisateur non-administrateur, mais certaines fonctions ne seront pas accessibles.

Droits du Registre

Pour créer un utilisateur non-administrateur, créez-en un et configurez les droits du Registre associés de la manière suivante.

- Accès complet à KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring
- Accès complet au répertoire CANDLE_HOME

L'utilisateur non-administrateur doit appartenir aux groupes Utilisateurs de l'Analyseur des performances et Utilisateurs du journal des performances. Si vous définissez ces autorisations pour un utilisateur non-administrateur, les données s'affichent pour tous les groupes d'attributs basés sur Perfmon.

Pour afficher les données des groupes d'attributs collectées de la base de données, procédez comme suit :

Si vous voulez afficher les données des groupes d'attributs collectées de la base de données, vous devez configurer les droits suivants pour l'utilisateur non-administrateur.

- Le compte utilisateur non-administrateur que vous utilisez pour exécuter l'Agent Skype for Business Server doit disposer du droit Déboguer les programmes pour pouvoir ajouter un débogueur à un processus.

Par défaut, le droit Déboguer les programmes est affecté uniquement aux comptes Administrateur et Système local. Pour accorder le droit Déboguer les programmes, vous devez exécuter les étapes suivantes sur le serveur Lync ou Skype for Business :

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre Propriétés de Déboguer les programmes apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

- Accordez le droit Ouvrir une session en tant que service

  Pour accorder le droit Ouvrir une session en tant que service, vous devez exécuter les étapes suivantes sur le serveur Lync ou Skype for Business :

  1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
  2. Dans le panneau de gauche, développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche dans le panneau de droite.
  3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre Propriétés de Ouvrir une session en tant que service apparaît.
  4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
  5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
  6. Cliquez sur **OK**.

Le groupe d'attributs Disponibilité affiche les données propres aux membres du groupe Administrateurs.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent Skype for Business Server (anciennement agent MS Lync Server) sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

L'Agent Skype for Business Server fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Skype for Business Server**, puis sur **Configuration de l'agent**.
3. Dans la fenêtre Monitoring Agent for Skype for Business Server, procédez comme suit :

a. Dans l'onglet **SQL Configuration for Skype for Business Topology**, pour vous connecter au Central Management Store de Microsoft Lync Server ou Skype for Business Server, indiquez des valeurs pour les paramètres de configuration, puis cliquez sur **Suivant**.

   Important : La configuration des transactions synthétiques est facultative. Si vous avez besoin des données de transaction synthétique, spécifiez les paramètres de configuration dans les onglets **Setup Information** et **Scheduler Configuration**.

b. Dans l'onglet **Administrator Login Credentials**, spécifiez les données d'identification de l'administrateur, puis cliquez sur **Suivant**.

c. Dans l'onglet **Setup Information**, pour exécuter les commandes des transactions synthétiques, indiquez des valeurs pour les paramètres de configuration, puis cliquez sur **Suivant**.

d. Dans l'onglet **Scheduler Configuration**, pour planifier les transactions synthétiques, spécifiez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.

e. Dans l'onglet **SQL Server Configuration for Skype for Business Monitoring Role**, pour vous connecter au rôle de surveillance de Microsoft Lync Server ou Skype for Business Server, indiquez des valeurs pour les paramètres de configuration, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 482.

4. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Skype for Business Server**, puis sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Lorsque vous installez l'Agent Skype for Business Server (anciennement agent MS Lync Server), l'agent est à l'état non configuré. Pour le démarrer, vous devez le configurer.
Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Avant de commencer

Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Procédure

Pour configurer l'Agent Skype for Business Server, procédez comme suit :

1. Ouvrez l'invite de commande.
2. Modifiez le chemin d'accès au répertoire qui contient le fichier `skype_for_business_server-agent.bat`.
3. Entrez la commande **`skype_for_business_server-agent.bat config`** *chemin absolu du fichier de réponses*.

Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent».

4. Démarrez l'agent s'il est à l'état arrêté.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Modification du compte utilisateur

Après avoir configuré l'Agent Skype for Business Server, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche

Par défaut, l'Agent Skype for Business Server s'exécute sous le compte utilisateur local. Lorsque l'agent s'exécute sous l'utilisateur de domaine, il peut collecter les données des serveurs distants.

Procédure

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent :
   ```
   rép_install\InstallITM\KinCinfo.exe –r
   ```
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre Manage Monitoring Services.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme <Domaine\ID_utilisateur>, puis indiquez le mot de passe.
6. Démarrez Agent Skype for Business Server.

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent Skype for Business Server (anciennement agent MS Lync Server), vous pouvez modifier les valeurs par défaut des paramètres de configuration, comme le nom du serveur de base de données, le nom de l'instance de base de données, le nom de la base de données et d'autres paramètres.

Le tableau ci-après contient les descriptions des paramètres de configuration de l'Agent Skype for Business Server.

Remarque : Aucune des zones du tableau ci-après n'est obligatoire.

Tableau 135. Noms et descriptions des paramètres de configuration de l'agent

Nom du paramètre	Description
Nom de serveur de base de données (par exemple, PS6877)	• Onglet **SQL Configuration for Skype for Business Topology** : nom du serveur de base de données sur lequel le Central Management Store de Lync ou Skype for Business Server est installé. • Onglet **SQL Server Configuration for Skype for Business Monitoring Role** : nom du serveur de base de données sur lequel le rôle de surveillance est installé.
Nom de l'instance de base de données	• Onglet **SQL Configuration for Skype for Business Topology** : nom de l'instance. • Onglet **SQL Server Configuration for Skype for Business Monitoring Role** : nom de l'instance de base de données sur laquelle le rôle de surveillance est installé.
Nom de la base de données	Nom de la base de données.
ID utilisateur de base de données	ID utilisateur de la base de données. Cet utilisateur doit disposer de droits d'accès à l'instance Microsoft SQL Server requise. Cet utilisateur n'a pas besoin d'être un utilisateur Active Directory.
Mot de passe Base de données	Mot de passe de la base de données dans laquelle le rôle de surveillance est installé.
ID utilisateur de domaine (par exemple, skype\administrator)	ID utilisateur de l'administrateur. Ce doit être un utilisateur de domaine disposant de privilèges d'administrateur et de droits d'accès à tous les serveurs distants répertoriés dans la topologie Lync ou Skype for Business Server.
Mot de passe de domaine	Mot de passe de l'administrateur.
Confirmer le mot de passe de domaine	Entrez le mot de passe indiqué dans la zone Mot de passe de domaine.
Nom de domaine complet	Nom de domaine complet (FQDN) du système de production.
Zone géographique	Zone géographique du système de production.
Utilisateur1 de test (par exemple, user1@skype.com)	Premier prénom que vous pouvez utiliser pour exécuter les commandes de transactions synthétiques.
Mot de passe Utilisateur1 de test	Mot de passe du premier utilisateur.
Utilisateur2 de test (par exemple, user2@skype.com)	Second nom d'utilisateur que vous pouvez utiliser pour exécuter les commandes de transactions synthétiques.
Mot de passe Utilisateur2 de test	Mot de passe du second utilisateur.
Fréquence	Fréquence d'exécution de l'utilitaire planifié qui extrait les données des transactions synthétiques. La fréquence peut avoir les valeurs suivantes : • Quotidien (DAY_FREQUENCY) • Hebdomadaire (WEEK_FREQUENCY) • Mensuel (MONTHLY_FREQUENCY)
Heure de collecte	Partie de l'horodatage représentant les heures, dans une horloge au format 24 heures que vous sélectionnez pour planifier l'exécution de l'utilitaire.
Minute de collecte	Partie de l'horodatage représentant les minutes, dans une horloge au format 24 heures que vous sélectionnez pour planifier l'exécution de l'utilitaire.
Date de début (AAAA-MM-JJ)	Date d'activation du planificateur.
Date de fin (AAAA-MM-JJ)	Date de désactivation du planificateur.

Configuration de la surveillance de Microsoft .NET

L'Monitoring Agent for Microsoft .NET surveille les applications .NET. Il démarre automatiquement après l'installation pour collecter les données de surveillance des ressources. Cependant, pour la collecte des données de diagnostic et de suivi des transactions, vous devez effectuer certaines tâches de configuration.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft .NET.

Pourquoi et quand exécuter cette tâche

Une fois que l'agent est installé, effectuez les tâches de configuration suivantes pour que l'agent puisse collecter les données de diagnostic et de suivi des transactions :

1. Enregistrement du collecteur de données
   Le collecteur de données est un composant de l'agent Microsoft .NET. Il collecte les données de suivi des transactions et de diagnostic et les envoie à l'agent Microsoft .NET. Vous devez enregistrer le collecteur de données pour la collecte de ces données. Pour plus d'informations, voir «Enregistrement du collecteur de données», à la page 485.
2. Configuration de la collecte des données de suivi des transactions et de diagnostic
   Après avoir enregistré le collecteur de données, activez la collecte des données de diagnostic et de suivi des transactions sur la console Cloud APM. Vous pouvez également activer la collecte des données de diagnostic à l'aide de la commande **configdc**. Pour plus d'informations, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 488 et «Activation de la collecte des données de diagnostic à l'aide de la commande configdc», à la page 489.
3. Activation des mises à jour de configuration
   Si vous activez la collecte de données de diagnostic à l'aide de la commande **configdc**, vous devez activer la configuration de telle sorte que les mises à jour soient sauvegardées dans le fichier de configuration. Pour plus d'informations sur l'activation des changements de configuration, voir «Activation des mises à jour de configuration», à la page 491.
4. Optimisation des performances du collecteur de données
   Vous pourriez avoir besoin d'effectuer certaines tâches pour réajuster les performances du collecteur de données. Pour plus d'informations, voir «Optimisation des performances du collecteur de données» , à la page 491.

Coexistence des agents
Dans un environnement de coexistence d'agent, vous pouvez afficher les données de suivi des transactions à partir de la console Cloud APM ou de Tivoli® Enterprise Portal. Pour plus d'informations sur l'activation de la collecte de données pour le suivi des transactions dans l'environnement de coexistence d'agent, voir «Activation du suivi des transactions dans l'environnement de coexistence d'agent», à la page 490.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 136. Versions d'agent et documentation

Version de l'agent Microsoft .NET	Documentation
8.1.3.2	IBM Cloud Application Performance Management
8.1.3 et 8.1.2	IBM Performance Management 8.1.3 *

* Le lien ouvre une rubrique Knowledge Center sur site.

Droits nécessaires pour exécuter un agent à l'aide d'un compte local ou de domaine

Seul un utilisateur local ou du domaine qui est membre du groupe Administrateurs est autorisé à exécuter l'agent Microsoft .NET. Cette rubrique fournit les conditions à remplir si l'utilisateur local ou du domaine n'est pas membre du groupe Administrateurs.

L'utilisateur doit disposer des droits suivants sur l'unité système et l'unité d'installation de l'agent :

1. Lecture
2. Ecriture
3. Exécution
4. Modification

L'utilisateur doit disposer du droit suivant sur la clé de registre HKEY_LOCAL_MACHINE

- Lecture

L'utilisateur doit être membre des groupes suivants sur le serveur surveillé :

1. Utilisateurs
2. IIS_IUSRS
3. Utilisateurs du moniteur de performances
4. Utilisateurs du journal de performances

Remarque : Il est toutefois conseillé d'exécuter l'agent Microsoft .NET avec un utilisateur local ou de domaine qui soit membre du groupe Administrateurs local.

Enregistrement du collecteur de données

Vous devez enregistrer le collecteur de données pour qu'il collecte les données de suivi des transactions et les données de diagnostic. Pour collecter les données de surveillance des ressources, aucune configuration spécifique n'est requise.

Pourquoi et quand exécuter cette tâche

Enregistrez les composants suivants du collecteur de données, en fonction du type de données (transaction et/ou diagnostics) que le collecteur de données doit collecter :

Tableau 137. Composants du collecteur de données et leurs fonctions

Nom du composant	Surveille
httpmodule	Les transactions ASP.NET et collecte le temps de réponse aux demandes et le temps UC
profiler	Les transactions ADO.NET et collecte les données de méthode, de trace de pile et de contexte de demande à des fins de diagnostic
isapi	Les transactions ASP.NET et collecte le temps de réponse aux demandes et le temps UC
soap	Les transactions de service ASMX ou WCF et le temps de réponse des services WCF

A faire :

- Utilisez `isapi32` pour filtrer les applications 32 bits sur un serveur Microsoft IIS Server 64 bits.
- Enregistrez tous les composants pour suivre toutes les transactions et affichez la topologie complète des transactions.

Procédure

1. Sur le serveur où l'agent est installé, exécutez la commande suivante en tant qu'administrateur :

   ```
   cd rép_install\qe\bin
   configdc.exe registerdc [all|isapi|isapi32|profiler|httpmodule|soap]
   ```

   A faire :

   - Lorsque vous exécutez la commande **configdc.exe registerdc** sans spécifier de composant à enregistrer, seul httpmodule est enregistré.
   - Pour enregistrer tous les composants, exécutez la commande **configdc.exe registerdc all**.
   - Pour enregistrer n'importe quels composants ensemble, exécutez cette commande : **configdc.exe registerdc** *nom_composant nom_composant*. Par exemple, **configdc.exe registerdc** httpmodule profiler
2. Redémarrez les applications .NET.

Que faire ensuite

Après avoir enregistré le collecteur de données, vous devez activer la collecte de données pour le suivi des transactions et les diagnostics. Pour plus d'informations sur l'activation de la collecte de données, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 488.

Si vous souhaitez arrêter la surveillance des applications .NET, annulez l'enregistrement du collecteur de données. Répétez les étapes indiquées en utilisant la commande **configdc.exe unregisterdc** pour annuler l'enregistrement de tous les composants du collecteur de données.

Utilisation du module de temps de réponse IIS de l'agent .NET

A partir de l'édition 8.1.4.0.2, l'agent .NET inclut le «module de temps de réponse IIS», qui fonctionne avec l'agent de temps de réponse pour afficher les données de transaction des utilisateurs finaux pour le serveur IIS.

Activation du module de temps de réponse

Vous devez activer le module de temps de réponse avant de l'utiliser.

Procédure

Pour activer le module de temps de réponse, procédez comme suit :

1. Ouvrez l'invite de commande en mode administrateur.
2. Pour arrêter IIS, exécutez la commande suivante :

   ```
   iisreset /stop
   ```
3. Accédez au répertoire `rép_install\qe\bin` à partir de l'invite de commande.
4. Pour enregistrer le module de temps de réponse pour IIS, exécutez la commande suivante :

   ```
   configdc registerdc rtmodule
   ```
5. Pour démarrer IIS, exécutez la commande suivante :

   ```
   iisreset /start
   ```

Résultats

Le module de temps de réponse est activé.

Configuration de l'agent de temps de réponse pour une utilisation avec le module de temps de réponse IIS de l'agent .NET

Vous devez configurer l'agent de temps de réponse pour l'utiliser avec le module de temps de réponse IIS de l'agent .NET.

Avant de commencer

Installez l'agent de temps de réponse (version 8.1.4). Pour plus d'informations, voir Chapitre 9, «Installation des agents», à la page 161.

Procédure

Pour configurer l'agent de temps de réponse pour l'utiliser avec le module de temps de réponse IIS de l'agent .NET, procédez comme suit :

1. Ouvrez un éditeur de texte en mode administrateur.
2. Ouvrez le fichier suivant dans un éditeur de texte :

   rép_config\TMAITM6_x64*nom_hôte*_T5.config

   où *rép_config* est le répertoire de base d'APM et *nom_hôte* est le nom du serveur.
3. Mettez à jour la propriété suivante :

   `{ KT5DISABLEANALYZER=YES } { KT5ENABLEWEBPLUGIN=YES }`
4. Ajoutez la propriété suivante dans la section `SECTION=analyzerconfig [ ]` :

   `{KT5WEBPLUGINIPCNAME=KFC1}`
5. Redémarrez l'agent de temps de réponse.
6. Connectez-vous à la console Performance Management pour vérifier les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Performance Management, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'injection JavaScript pour le module de temps de réponse IIS

Vous devez configurer l'injection JavaScript (JS) pour qu'elle fonctionne avec le module de temps de réponse IIS (Internet Information Services) de l'agent .NET.

Procédure

Pour configurer l'injection JS de sorte qu'elle fonctionne avec le module de temps de réponse IIS de l'agent .NET, procédez comme suit :

1. Ouvrez un éditeur de texte en mode administrateur.
2. Ouvrez le fichier suivant dans un éditeur de texte :

   `<APM_HOME>\qe\config\dotNetDcConfig.properties.inactive`
3. Pour activer l'injection JS pour le module de temps de réponse, définissez la propriété **`RTModule.JSInjection.Enabled`** sur **`true`**.
4. Pour désactiver l'injection JS pour le module de temps de réponse, définissez la propriété **`RTModule.JSInjection.Enabled`** sur **`false`**.
5. Ouvrez l'invite de commande en mode administrateur, puis accédez au répertoire `<APM_HOME>\qe\bin`.
6. Exécutez les commandes suivantes :
   - `configdc activateconfig`
   - `iisreset`

Désactivation du module de temps de réponse IIS

Vous pouvez désactiver le module de temps de réponse IIS lorsque vous ne souhaitez plus afficher les données de transaction des utilisateurs finaux pour le serveur IIS.

Procédure

Pour désactiver le module de temps de réponse IIS, procédez comme suit :

1. Ouvrez l'invite de commande en mode administrateur.
2. Pour arrêter IIS, exécutez la commande suivante :
   ```
   iisreset /stop
   ```
3. Accédez au répertoire *rép_install*\qe\bin à partir de l'invite de commande.
4. Pour annuler l'enregistrement du module de temps de réponse pour ISS, procédez comme suit :
   - Exécutez la commande suivante :
     ```
     configdc unregisterdc rtmodule
     ```
   - Pour annuler l'enregistrement de tous les composants du collecteur de données, y compris le module de temps de réponse, exécutez la commande suivante :
     ```
     configdc unregisterdc all
     ```
5. Pour démarrer IIS, exécutez la commande suivante :
   ```
   iisreset /start
   ```

Résultats

Le module de temps de réponse IIS est désactivé.

Limitations du module de temps de réponse IIS

Les limitations du module de temps de réponse IIS sont répertoriées ici.

- Les informations utilisateur ne sont pas suivies par le module de temps de réponse IIS et le nom d'utilisateur affiché est actuellement «Unknown».

Activation de la collecte des données de suivi des transactions et de diagnostic

Sur la page Configuration d'agent, vous pouvez activer ou désactiver la collecte des données de suivi des transactions et de diagnostic.

Avant de commencer

Vérifiez que vous avez enregistré le collecteur de données. Pour plus d'informations, voir «Enregistrement du collecteur de données», à la page 485.

Procédure

Procédez comme suit pour configurer la collecte des données pour chaque système géré.

1. Connectez vous à console Cloud APM.
2. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
3. Cliquez sur l'onglet **MS .NET**.
4. Cochez les cases des systèmes gérés pour lesquels vous voulez configurer la collecte de données et effectuez l'une des actions suivantes de la liste **Actions**.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking (Définir le suivi des transactions)** > **Activé**. Le statut de la colonne **Transaction Tracking** est mis à jour sur Enabled pour chaque système géré sélectionné.
   - Pour activer la collecte des données de diagnostic, sélectionnez **Set Diagnostic Mode** (Définir le mode diagnostic) et cliquez sur le niveau de votre choix. Le statut indiqué dans la colonne **Diagnostic Mode** est mis à jour de manière à afficher le niveau spécifié pour chaque système géré sélectionné.

  - Niveau 1 : Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes.
  - Niveau 2 : Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes. Le profileur collecte les données de méthode et de trace de pile.
- Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Désactivé**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.
- Pour désactiver la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Disabled**. Le statut indiqué dans la colonne **Diagnostic Mode** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.

Résultats

La collecte de données est configurée pour chaque système géré.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données de suivi des transactions et de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Activation de la collecte des données de diagnostic à l'aide de la commande configdc

Vous pouvez également activer ou désactiver la collecte des données de diagnostic à l'aide de la commande **configdc**. Ce processus est facultatif.

Avant de commencer

- Vérifiez que vous avez enregistré le collecteur de données. Pour plus d'informations, voir «Enregistrement du collecteur de données», à la page 485.
- Assurez-vous d'avoir effectué la procédure «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 488.
- Vérifiez que le fichier `qe_custom.properties` est traité par le serveur APM dans `<APM_Home>\localconfig\qe` et qu'il contient les propriétés suivantes :
  - transaction_tracking=ENABLED
  - diagnostic_mode=LEVEL2

Procédure

1. Exécutez la commande suivante :

   ```
   cd rép_install\qe\bin configdc deepdivedc -tracelevel niveau_trace
   ```

   Où,

   rép_install
   Répertoire d'installation de l'agent Microsoft .NET.

   niveau_trace
   Niveau de trace qui indique la quantité de données de diagnostic collectées par l'.NET Data Collector. Spécifiez l'une des valeurs suivantes :

   0 La collecte des données de diagnostic est désactivée.

   1 La collecte des données de diagnostic est activée. Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes.

2 La collecte des données de diagnostic est activée. Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes. Le profileur collecte les données de méthode et de trace de pile.

Conseil : La définition du niveau de trace en utilisant la commande **configdc.exe deepdivedc -tracelevel** définit la valeur du paramètre `bci_dc.diagnose.level` dans le fichier `dotNetDcConfig.properties`.

2. Activez les changements de configuration. Pour plus d'informations sur l'activation des modifications, voir «Activation des mises à jour de configuration», à la page 491.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Activation du suivi des transactions dans l'environnement de coexistence d'agent

Dans un environnement de coexistence d'agent, vous pouvez configurer le collecteur de données pour collecter et transmettre les données de suivi des transactions à Tivoli Enterprise Portal, qui est un composant d'IBM Tivoli Monitoring.

Avant de commencer

Vous devez installer l'agent Microsoft .NET, qui est fourni dans Cloud APM et vous devez supprimer ou désenregistrer le composant .NET Data Collector, qui est fourni avec ITCAM for Microsoft Applications. Utilisez la commande **configdc.exe unregisterdc** pour désenregistrer tous les modules du collecteur de données.

Procédure

Pour configurer le collecteur de données dans le but de collecter et de transmettre les données de suivi des transactions à Tivoli Enterprise Portal, procédez comme suit :

1. Accédez au répertoire *rép_install*`\localconfig\qe`, où *rép_install* est le répertoire d'installation de l'agent Microsoft .NET. Le chemin par défaut est `C:\IBM\APM`.
2. Ouvrez le fichier `qe_default.properties` et définissez la valeur du paramètre **transaction_tracking** sur `ENABLED`.
3. Sauvegardez et fermez le fichier `qe_default.properties`.
4. Accédez au répertoire *rép_install*`\qe\config`.
5. Ouvrez le fichier `dotNetDcConfig.properties.inactive` dans un éditeur de texte.
6. Définissez les paramètres **TTDC.enabled** et **TTAS.enabled** comme suit :

   ```
   TTDC.enabled=true
   TTAS.enabled=true
   ```

7. Pour configurer la connexion au collecteur de transactions, affectez l'adresse IP et le numéro de port du collecteur de transactions aux paramètres **TTAS.Host** et **TTAS.Port**.
8. Exécutez la commande suivante pour activer les changements :

   rép_install`\qe\bin\configdc.exe activateconfig`

9. Redémarrez l'application .NET pour appliquer les changements.

Résultats

Les données de suivi des transactions peuvent être collectées et affichées dans Tivoli Enterprise Portal.

Que faire ensuite

Pour désactiver l'opération de suivi pour un .NET Data Collector, répétez la procédure et utilisez les valeurs de configuration suivantes :

- Dans le fichier `qe_default.properties`, définissez `transaction_tracking=DISABLED`.
- Dans le fichier `dotNetDcConfig.properties.inactive`, définissez `TTDC.enabled=false` et `TTAS.enabled=false`.

Activation des mises à jour de configuration

Vous devez activer les mises à jour que vous effectuez dans les paramètres de configuration à l'aide de la commande `configdc`. Cette activation permet de sauvegarder vos mises à jour dans le fichier `dotNetConfig.properties`.

Pourquoi et quand exécuter cette tâche

Lorsque vous mettez à jour les paramètres de configuration à l'aide de la commande **`configdc`**, les valeurs des paramètres sont mises à jour dans le fichier `dotNetConfig.properties`. Toutefois, si ce fichier est déjà utilisé et qu'il ne peut pas être modifié, vos mises à jour des paramètres de configuration sont sauvegardées dans le fichier `dotNetDcConfig.properties.inactive`. Vous devez activer la configuration de sorte que les mises à jour soient sauvegardées dans le fichier `dotNetConfig.properties`.

Procédure

1. Accédez au chemin suivant :
   rép_install`\qe\bin`
   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Exécutez la commande suivante :
   `configdc activateConfig`

Que faire ensuite

Si les transactions IIS (Internet Information Service) sont surveillées et que la configuration du collecteur de données est mise à jour, redémarrez IIS pour activer la configuration.

Si les services Web ASMX ou WCF sont surveillés et que la configuration du collecteur de données est mise à jour, redémarrez le processus hébergeant le service Web.

Optimisation des performances du collecteur de données

Lorsque vous configurez le collecteur de données pour qu'il collecte les données de suivi des transactions et de diagnostic, les performances du collecteur de données en sont affectées. Pour améliorer les performances, vous pouvez effectuer certaines tâches d'optimisation des performances.

Vous pourriez avoir besoin d'effectuer les tâches suivantes pour améliorer les performances du collecteur de données :

- Filtrer les interfaces ADO.NET que vous voulez surveiller.
- Echantillonner les données de suivi des transactions et de diagnostic.
- Configurer la consignation de trace.

Spécification d'interfaces ADO.NET pour la surveillance

Vous pouvez indiquer les interfaces client ADO.NET à activer pour le suivi des transaction.

Avant de commencer

Pour afficher les interfaces ADO.NET prises en charge par .NET Data Collector, voir Functions of namespaces supported by the data collector.

Pour afficher les valeurs de configuration de l'.NET Data Collector, consultez le fichier `dotNetDcConfig.properties` dans le répertoire *rép_install*`\qe\config`, où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.

Pourquoi et quand exécuter cette tâche

Par défaut, toutes les interfaces ADO.NET prises en charge sont activées pour le suivi des transactions lors de l'installation de l'agent. Pour spécifier les interfaces que doit surveiller le collecteur de données, activez ou désactivez la surveillance pour des interfaces spécifiques.

Si vous désactivez la surveillance d'une interface, les paramètres des filtres de domaine d'application associés sont conservés dans le fichier de configuration du collecteur de données. Le filtre est conservé lorsque l'interface est réactivée.

Procédure

- Pour activer la surveillance d'une interface ADO.NET, procédez comme suit :
  1. Depuis le répertoire *rép_install*`\qe\bin`, exécutez la commande suivante :
     ```
     configdc enableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
     | http | web
     [-appdomain liste filtres domaineapp]
     ```
  2. Activez les changements de configuration. Pour plus d'informations sur l'activation des modifications, voir «Activation des mises à jour de configuration», à la page 491.
- Pour désactiver la surveillance d'une interface ADO.NET, procédez comme suit :
  1. Depuis le répertoire *rép_install*`\qe\bin`, exécutez la commande suivante :
     ```
     configdc disableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
     | http | web
     ```
  2. Activez les changements de configuration. Pour plus d'informations sur l'activation des modifications, voir «Activation des mises à jour de configuration», à la page 491.

Echantillonnage de données de diagnostic et de suivi des transactions

Si les performances du système sont affectées en raison de la collecte des données de suivi des transactions ou de diagnostic, vous pouvez activer l'échantillonnage des données collectées afin d'améliorer les performances.

Pourquoi et quand exécuter cette tâche

Lorsque la performance du système pâtit du suivi des transactions et de la collecte des données de diagnostic, vous pouvez configurer le collecteur de données pour collecter périodiquement des données par échantillonnage. Lorsque l'échantillonnage est activé, le collecteur de données ne collecte pas les données pour chaque demande, mais à intervalles de plusieurs demandes. Vous pouvez modifier la fréquence d'échantillonnage de manière dynamique en fonction de l'utilisation de l'unité centrale par le processus DotNetProfilerService.

ATTENTION :
L'échantillonnage permet d'épargner des ressources système, mais les données d'échantillon risquent de ne pas suffire pour diagnostiquer des problèmes. Par ailleurs, une fois l'échantillonnage de données activé, la topologie de suivi des transactions peut être détériorée ou perdue. Par conséquent, n'activez l'échantillonnage de données que si les performances sont sérieusement affectées.

Procédure

Pour activer l'échantillonnage sur la collecte des données de diagnostic et de suivi des transactions, procédez comme suit :

1. Accédez au répertoire suivant :
   rép_install\qe\config
   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Dans un éditeur de texte, ouvrez le fichier dotNetDcConfig.properties.inactive.
3. Dans ce fichier, définissez de manière appropriée les paramètres suivants :

   bci_dc.sampling.Enabled
   Indique si le collecteur de données collecte régulièrement des données de diagnostic et de suivi des transactions. Les valeurs admises sont true et false.

   bci_dc.sampling.base
   Indique la base de l'échantillonnage de données. Les valeurs admises sont les nombres positifs. Par exemple, si vous définissez la valeur du paramètre **bci_dc.sampling.base** sur 10, le collecteur de données recueille les données de diagnostic et de suivi des transactions toutes les 10 demandes. La fréquence d'échantillonnage est de 1 sur 10 demandes. Le collecteur de données collecte des données pour les 1re, 11e, 21e, 31e, etc. demandes.

   bci_dc.dynamic.sampling
   Indique si la fréquence d'échantillonnage est constante ou dynamique. Les valeurs admises sont on et off. Lorsque vous définissez la valeur du paramètre **bci_dc.dynamic.sampling** sur on, le taux d'échantillonnage est ajusté de manière dynamique en fonction de la valeur du paramètre **bci_dc.dynamic.max_cpu_usage**.

   bci_dc.dynamic.max_cpu_usage
   Indique le seuil d'utilisation de l'unité centrale pour le processus DotNetProfilerService. Si l'utilisation de l'unité centrale par le processus DotNetProfilerService est supérieure à 110 % de la valeur indiquée, la fréquence d'échantillonnage est réduite. Si l'utilisation de l'unité centrale est inférieure à 90 % de la valeur indiquée, la fréquence d'échantillonnage est augmentée. Les valeurs admises sont comprises entre 1 et 100.
4. Sauvegardez et fermez le fichier dotNetDcConfig.properties.inactive.
5. Exécutez la commande suivante pour activer les modifications :
   rép_install\qe\bin\configdc.exe activateconfig
6. Redémarrez l'application .NET pour appliquer la modification.

Activation de la consignation de trace pour le collecteur de données

Vous pouvez activer la génération de journaux de trace pour le collecteur de données. Vous pouvez utilisez ces journaux de trace pour traiter les incidents qui pourraient se produire avec la collecte des données de suivi des transactions et de diagnostic.

Pourquoi et quand exécuter cette tâche

Pour collecter les journaux des transactions ASP.NET, ADO.NET et des données de diagnostic, activez les journaux de trace pour httpmodule, le profileur et les composants isapi du collecteur de données. Pour collecter les journaux des transactions ASMX et WCF, activez les journaux de trace du composant soap du collecteur de données.

Important : Les performances du collecteur de données peuvent être affectées lorsque la consignation de trace est activée. Par conséquent, désactivez la consignation de trace une fois le journaux de trace collectés.

Procédure

1. Sur le serveur où l'agent est installé, accédez au répertoire suivant :
   rép_install\qe\bin où *rép_install* est le répertoire d'installation de l'agent Microsoft .NET.
2. Effectuez les deux procédures suivantes ou l'une d'entre elles en fonction des journaux de trace que vous voulez activer :
   - Pour activer les journaux de trace pour httpmodule, le profileur, les composants SOAP et le module de temps de réponse, procédez comme suit :
     a. Exécutez la commande suivante :
        configdc logging -tracing on
     b. Redémarrez les applications IIS et .NET.
   - Pour activer les journaux de trace pour le moteur BCI, procédez comme suit :
     a. Accédez au chemin suivant :
        <APM_HOME>\qe\config
     b. Dans un éditeur de texte, ouvrez le fichier dotNetDcConfig.properties.inactive.
     c. Pour le propriété **bci_dc.trace.logging**, spécifiez la valeur on.
     d. Exécutez la commande suivante :
        configdc activateconfig
     e. Redémarrez IIS.

Que faire ensuite

Pour désactiver les journaux de trace, procédez comme suit :

- Pour désactiver les journaux de trace pour httpmodule, le profileur, les composants SOAP et le module de temps de réponse, procédez comme suit :
  – Exécutez la commande suivante :
    configdc logging -tracing off
  – Redémarrez les applications IIS et .NET.
- Pour désactiver les journaux de trace pour le moteur BCI :
  – Accédez au chemin suivant :
    <APM_HOME>\qe\config
  – Dans un éditeur de texte, ouvrez le fichier dotNetDcConfig.properties.inactive.
  – Pour la propriété **bci_dc.trace.logging**, spécifiez la valeur off.
  – Exécutez la commande suivante :
    configdc activateconfig
  – Redémarrez les applications IIS et .NET.

Configuration de la surveillance de Microsoft Office 365

Vous devez configurer agent Microsoft Office 365 pour surveiller la disponibilité et les performances des abonnements Microsoft Office 365 de l'organisation.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel.
- Pour collecter des données pour les utilisateurs Office 365, il faut que les modules suivants soient installés sur le client Windows où l'agent est installé :
  – PowerShell 3.0 ou version ultérieure
  – Microsoft Online Services Sign-In Assistant PowerShell
  – SharePoint Online Management Shell
  – DotNetFrameworkVersion 4.5.2 ou version ultérieure

– Azure Active Directory PowerShell

Un utilisateur qui configure l'agent doit disposer des privilèges d'administration avec des privilèges pour activer la règle d'exécution à distance de PowerShell.

- Pour surveiller les transactions synthétiques Skype, effectuez les tâches suivantes :
  – Installez le client Skype 2013 sur le client Windows sur lequel l'utilisateur veut exécuter des transactions synthétiques pour Skype.
  – Définissez le périphérique vidéo par défaut pour Lync et Skype comme filtre audio/vidéo virtuel.
- Vérifiez que l'utilisateur qui démarre Microsoft Office 365 dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Office 365.

Pourquoi et quand exécuter cette tâche

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir agent Microsoft Office 365. Pour accéder à la documentation de la version 1.0.0, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management.

Vous pouvez démarrer l'agent Microsoft Office 365 une fois installé. Une configuration manuelle est toutefois requise pour afficher les données pour tous les attributs d'agent.

Pour configurer l'agent, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.

Vérification de l'accessibilité des utilisateurs configurés

Pour vérifier l'accessibilité, l'agent Microsoft Office 365 envoie un message électronique aux utilisateurs configurés et mesure le temps nécessaire pour recevoir une réponse automatique. Avant de démarrer l'agent, vous devez configurer tous les utilisateurs, qui sont configurés dans les paramètres d'accessibilité de la boîte aux lettres de l'agent Office 365,pour répondre automatiquement aux messages électroniques.

Avant de commencer

Avant de configurer les utilisateurs Exchange Online pour l'accessibilité, vérifiez que les tâches suivantes ont été effectuées :

- Une boîte aux lettres est créée pour chaque utilisateur sur l'instance Exchange Online que vous souhaitez surveiller.
- L'utilisateur que vous avez créé pour l'agent est un utilisateur Office 365 global.

Procédure

Effectuez les étapes suivantes pour chaque compte utilisateur Exchange Online pour lequel vous souhaitez vérifier l'accessibilité :

1. Connectez-vous à Microsoft Outlook en indiquant les données d'identification de l'utilisateur que vous avez créé.
2. Cliquez sur **Outils > Règles et alertes > Nouvelle règle**.
3. Dans l'**assistant de règles**, sous **Commencer à partir d'une règle vide**, cliquez sur **Apply rule on messages I receive**, puis sur **Suivant**.

4. Sélectionnez les options suivantes :
   - **From people or public group**
   - **Qui contiennent des mots spécifiques dans l'objet**
5. Sous **Etape 2** dans cette fenêtre, cliquez sur **people or public group**.
6. Dans la fenêtre **Rule address**, sélectionnez l'utilisateur (administrateur global) à partir duquel les messages doivent être reçus et cliquez sur **Next**.
7. Sous **Etape 2** dans cette fenêtre, cliquez sur **Mots spécifiques**.
8. Dans la zone **Spécifier un mot/une expression à rechercher dans l'objet/le corps du texte**, entrez `Tester l'accessibilté`.
9. Cliquez sur **Ajouter**.
10. Cliquez sur **OK**, puis sur **Suivant**.
11. Sélectionnez **Faire répondre le serveur avec un message spécifique** et cliquez sur **un message spécifique**.
12. Dans l'éditeur de message électronique, entrez le texte suivant dans la zone d'objet du message : `Tester l'accessibilité`.
13. Dans la liste **To**, ajoutez l'administrateur global.
14. Fermez l'éditeur de message électronique et cliquez sur **Oui** pour sauvegarder ces modifications.
15. Cliquez sur **Terminer**.
16. Cliquez sur **Appliquer**, puis sur **OK**.

Que faire ensuite

Configurez l'agent Microsoft Office 365.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Microsoft Office 365 sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

L'agent Microsoft Office 365 fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez à l'aide du bouton droit de la souris sur **Agent de surveillance pour Microsoft Office 365**, puis cliquez sur **Configuration de l'agent**.
3. Dans la fenêtre Agent de surveillance pour Microsoft Office 365, procédez comme suit :
   a. Dans l'onglet **Détails de l'abonnement Office365**, entrez le nom d'utilisateur et le mot de passe de l'administrateur global Office 365, puis cliquez sur **Suivant**.
   b. Dans l'onglet **Transaction synthétique**, entrez la liste des adresses e-mail délimitées par des points-virgules dans la zone **Reachability Email Addresses**.

c. Pour activer la collecte des mesures de qualité de service Skype, sélectionnez la case à cocher **Skype QoS** et cliquez sur **Suivant**.
d. A partir de l'onglet **Mailbox and OneDrive Usage Monitoring**, sélectionnez la durée (en heures) pour l'intervalle de collecte dans la liste **Collection Interval**, puis cliquez sur **Suivant**.

4. Dans la fenêtre Monitoring Agent for Microsoft Office 365, cliquez sur **Yes**.

Que faire ensuite

- Configurez les fonctionnalités de transaction synthétique Skype pour surveiller les transactions synthétiques de qualité de service Skype. Pour plus d'informations sur la surveillance de la qualité de service Skype, voir «Surveillance de la qualité de service Skype», à la page 498.
- Modifiez le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour plus d'informations, voir «Modification du compte utilisateur», à la page 498.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.
- Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Lorsque vous installez l'agent Microsoft Office 365, il doit être configuré et démarré manuellement après avoir défini les paramètres de configuration. Utilisez le fichier de réponses silencieux pour configurer les paramètres personnalisés.

Avant de commencer

Editez le fichier de réponses pour modifier les paramètres de configuration par défaut suivants :

KMO_USER_NAME
Nom d'utilisateur de l'administrateur global Office 365.

KMO_PASSWORD
Mot de passe de l'administrateur global Office 365.

KMO_MAIL_ADDRESSES1
Liste des adresses e-mail à cibler pour vérifier l'accessibilité de la boîte aux lettres. La liste d'adresses e-mail doit être délimitée à l'aide de point-virgules.

KMO_SKYPE
Ce paramètre permet d'activer la collecte des transactions synthétiques de qualité de service Skype.

KMO_DATA_COLLECTION_DURATION
Durée (en heures) pendant laquelle l'agent attend d'extraire les données d'utilisation de la boîte aux lettres et de OneDrive.

Le fichier de réponses se trouve à l'emplacement suivant :
`<CANDLEHOME>\samples`

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Procédure

Pour configurer l'agent Microsoft Office 365, procédez comme suit :

1. A l'invite de commande, accédez au répertoire qui contient le fichier `microsoft_office365-agent.bat`.
2. Entrez la commande `microsoft_office365-agent.bat` *chemin d'accès absolu au fichier de réponses*.
   Le fichier de réponses contient les paramètres suivants :
3. Si l'agent est arrêté, démarrez-le.

Que faire ensuite

- Configurez les fonctionnalités de transaction synthétique Skype pour surveiller les transactions synthétiques de qualité de service Skype. Pour plus d'informations sur la surveillance de la qualité de service Skype, voir «Surveillance de la qualité de service Skype».
- Modifiez le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour plus d'informations, voir «Modification du compte utilisateur».
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.
- Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft Office 365, modifiez le compte utilisateur d'utilisateur local en utilisateur de domaine.

Pourquoi et quand exécuter cette tâche

Par défaut, l'agent Microsoft Office 365 s'exécute sous le compte utilisateur local.

Procédure

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent :
   rép_install\InstallITM\KinCinfo.exe –r
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre Manage Monitoring Services.
4. Dans la fenêtre Manage Monitoring Services, cliquez avec le bouton droit sur l'instance de l'agent et cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme <Domaine\ID_utilisateur>, puis indiquez le mot de passe.
6. Démarrez agent Microsoft Office 365.

Surveillance de la qualité de service Skype

Pour surveiller la qualité de service Skype, un utilisateur doit configurer les utilitaires de gestion des transactions synthétiques Skype, `kmoskypecaller.exe` et `Kmoskypereceiver.exe`, sur le client Windows où l'agent est installé ou dans un environnement distribué où le client Skype for Business est configuré.

Avant de commencer

Pour exécuter des transactions synthétiques, vous devez mettre à jour le nom d'appelant et le nom de destinataire Skype dans le fichier `<CANDLEHOME>\tmaitm6_x64\kmoskypecallerlist.properties` au format suivant :

```
appelant skype = destinataire skype
```

Par exemple, john@xyz.com = alan@xyz.com
Vous pouvez ajouter plusieurs destinataires d'appel Skype pour un seul appelant Skype au format suivant :
`appelant skype = liste de destinataires skype`
Par exemple, john@xyz.com = alam@xyz.com;bill@xyz.com;chuk@xyz.com

A faire : Si vous ne souhaitez pas exécuter de transactions synthétiques, mais que vous voulez surveiller la qualité de service Skype pour les utilisateurs en temps réel, la mise à jour du fichier `<CANDLEHOME>\TMAITM6_x64\kmoskypecallerlist.properties` n'est pas nécessaire.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent Microsoft Office 365 est configuré et démarré, les fichiers et dossiers suivants sont créés dans le répertoire `<CANDLEHOME>\TMAITM6_x64\` :

- `kmoskypecaller.properties`
- `kmoskypecallerlist.properties`
- `KMOSynthTransSkype.zip`
- `KMOSkypeTransReceiver.zip`

En outre, le fichier `kmoskypecaller.properties` est mis à jour avec l'IP et le port de serveur qui sont utilisés pour la communication entre l'agent et l'utilitaire kmoskypecaller.

Procédure

Pour configurer l'appelant Skype et les destinataires Skype et lancer des transactions synthétiques, telles que la messagerie instantanée, les appels audio et vidéo, et les sessions de partage d'application, effectuez les étapes suivantes :

1. Démarrez l'agent Office 365.
2. Copiez le fichier `KMOSynthTransSkype.zip` du client d'agent vers le client Windows à partir duquel l'appel Skype doit être initié.
3. Procédez à l'extraction du fichier `KMOSynthTransSkype.zip`.
4. Copiez le fichier `kmoskypecaller.properties` du client d'agent vers le dossier `KMOSynthTransSkype` extrait sur le client Windows à partir duquel l'appel Skype doit être initié.
5. Copiez le fichier `KMOSkypeTransReceiver.zip` à partir du client d'agent sur tous les clients Windows sur lesquels les appels Skype doivent être reçus.
6. Extrayez le fichier `KMOSkypeTransReceiver.zip` sur tous les clients Windows sur lesquels les appels Skype doivent être reçus, et exécutez `KMOSkypeTransReceiver.exe` pour lancer la réception de messages.
7. Pour initier les transactions synthétiques, exécutez le fichier `KMOSynthTransSkype.exe`, qui est disponible dans le dossier d'extraction `KMOSynthTransSkype` sur le client Windows. L'agent Office 365 doit commencer à recevoir les données de surveillance Skype du client appelant.

Résultats

L'agent démarre la surveillance de la qualité de service Skype.

Définition des variables d'environnement local

Vous pouvez définir les variables d'environnement local pour modifier le comportement de agent Microsoft Office 365.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.

2. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Advanced > Edit ENV File**.
3. Dans le fichier des variables d'environnement, entrez les valeurs pour les variables d'environnement.

   Pour plus d'informations sur les variables d'environnement que vous pouvez configurer, voir «Variables d'environnement local».

Variables d'environnement local

Vous pouvez changer le comportement de agent Microsoft Office 365 en définissant les variables d'environnement local.

Variables permettant de définir la méthode de collecte des données pour l'agent

Pour définir la méthode de collecte de données pour l'agent, utilisez les variables d'environnement suivantes :

- **CDP_DP_INITIAL_COLLECTION_DELAY** : cette variable permet de définir l'intervalle (en secondes) après lequel le pool d'unités d'exécution commence sa collecte de données.
- **KMO_MAILBOX_REACHABILITY_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour le groupe d'attributs d'accessibilité de la boîte aux lettres.
- **KMO_SKYPE_REPORT_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en heures) pour la fonction de statistiques d'utilisation de Skype for Business.
- **KMO_SERVICE_API_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de santé du service Office 365.
- **KMO_NETWORK_CONNECTION_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de connectivité Internet.
- **KMO_NETWORK_PERFORMANCE_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de performances réseau des services Office 365.
- **KMO_SITE_CONNECTION_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de connectivité Office 365.
- **KMO_SPSITE_COLLECTION_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de détails SharePoint Sites.
- **KMO_UASGE_STATS_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en heures) pour la fonction de statistiques sur l'utilisateur et l'utilisation des services Office 365.
- **KMO_TENANT_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de détails du titulaire Office 365.
- **KMO_ONEDRIVE_CONNECTIVITY_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de connectivité Office 365 OneDrive.
- **KMO_TENANT_DOMAIN** : cette variable permet de définir le nom de domaine du titulaire.

Configuration de la surveillance de Microsoft SharePoint Server

Lorsque vous installez l'Monitoring Agent for Microsoft SharePoint Server, il est configuré automatiquement avec les paramètres de configuration par défaut. Utilisez le fichier de réponses silencieux pour modifier les paramètres de configuration par défaut.

Avant de commencer

Veillez à exécuter les tâches suivantes :

- Vérifiez que l'utilisateur, qui se connecte à l'environnement ou à l'application Microsoft SharePoint Server, dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

A faire : Pour configurer l'agent Microsoft SharePoint Server, vous pouvez utiliser un utilisateur local ou un utilisateur de domaine à condition que celui-ci dispose des privilèges d'administrateur.

- Editez le fichier de réponses et modifiez les paramètres de configuration par défaut.

  Le fichier de réponses contient les paramètres suivants :

  KQP_DB_User
  ID utilisateur de la base de données.

  KQP_DB_Password
  Mot de passe de la base de données.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft SharePoint Server.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 138. Versions d'agent et documentation

Version de l'agent Microsoft SharePoint Server	Documentation
06.31.09.00, 06.31.10.00	IBM Cloud Application Performance Management
06.31.09.00	IBM Performance Management 8.1.3 *
06.31.07.00	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Procédure

Pour configurer l'agent Microsoft SharePoint Server, procédez comme suit :

1. Ouvrez l'invite de commande.
2. Modifiez le chemin d'accès au répertoire qui contient le fichier `ms_sharepoint_server-agent.bat`.
3. Entrez la commande **`ms_sharepoint_server-agent.bat config`** *chemin d'accès absolu au fichier de réponses*
4. Si l'agent est arrêté, démarrez-le.

Que faire ensuite

Après avoir configuré l'agent, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour connaître les étapes de modification du compte utilisateur, voir «Modification du compte utilisateur».

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft SharePoint Server, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent s'exécute sous l'utilisateur de domaine, il peut surveiller tous les composants du agent Microsoft SharePoint Server.

Procédure

Pour modifier le compte utilisateur, procédez comme suit :

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent. **rép_install\InstallITM\KinCinfo.exe –r**
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre Manage Monitoring Services.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme : `<Domaine\ID_Utilisateur>`, puis spécifiez le mot de passe.
6. Démarrez l'agent de surveillance.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Exécution de Monitoring Agent for Microsoft SharePoint Server en tant qu'utilisateur non-administrateur

Des stratégies de sécurité locales sont disponibles pour permettre à un utilisateur non-administrateur d'exécuter un Monitoring Agent for Microsoft SharePoint Server.

Pourquoi et quand exécuter cette tâche

La combinaison des deux stratégies de sécurité locales suivantes permet à un utilisateur non-administrateur d'exécuter l'agent Microsoft SharePoint Server :

1. Déboguer les programmes.
2. Ouvrir une session en tant que service.

Suivez la procédure fournie pour accorder des droits de sécurité locaux à un utilisateur non-administrateur.

Procédure

1. Accédez à TEMA et définissez les paramètres de démarrage de l'agent Microsoft SharePoint Server pour un utilisateur non-administrateur.
2. Ajoutez l'utilisateur non-administrateur dans le répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server` sous la clé de Registre et accordez des droits en lecture au répertoire.
3. Ajoutez l'utilisateur non-administrateur dans le répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions` sous la clé de Registre et accordez des droits en lecture à ce répertoire.
4. Ajoutez manuellement l'utilisateur non-administrateur dans le répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\16.0\Secure\` sous la clé de Registre et accordez des droits en lecture à ce répertoire.
5. Ajoutez l'utilisateur non-administrateur dans le répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` sous la clé de Registre et accordez des droits d'accès complets à ce répertoire.
6. Ajoutez l'utilisateur non-administrateur dans le répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib` sous la clé de Registre et accordez des droits en lecture à ce répertoire.

7. Ajoutez l'utilisateur non-administrateur dans le dossier d'installation de l'agent SharePoint (le dossier Candle, par exemple, `C:\IBM\APM`) et accordez des droits d'accès complets à ce dossier.
8. Exécutez la commande **secpol.msc** dans le **menu Démarrer** pour ouvrir la Stratégie de sécurité locale.
9. Pour ajouter l'utilisateur non-administrateur à la stratégie de sécurité locale, voir «Droits de la stratégie de sécurité locale».
10. Ajoutez l'utilisateur non-administrateur au groupe d'utilisateurs Connexion à SQL Server. L'utilisateur doit disposer des droits du rôle sysadmin SQL Server sur le serveur SQL Server.
11. Redémarrez l'agent Microsoft SharePoint Server.
12. Vérifiez le statut de l'agent Microsoft SharePoint Server et les données sur le portail APM.
13. Les groupes d'attributs suivants affichent les données relatives aux utilisateurs qui sont membres du groupe Administrateurs.
    a. Disponibilité
    b. Service Web

Droits de la stratégie de sécurité locale

Des stratégies de sécurité locales sont disponibles pour qu'un utilisateur non-administrateur puisse exécuter un agent Microsoft SharePoint Server. Ces stratégies permettent de démarrer, d'arrêter, de configurer l'agent ou d'en vérifier les données. Vous trouverez ci-dessous deux stratégies de sécurité locales grâce auxquelles un utilisateur non-administrateur peut exécuter l'agent Microsoft SharePoint Server :

Octroi du droit Ouvrir une session en tant que service

Vous pouvez accorder le droit Ouvrir une session en tant que service.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Ouvrir une session en tant que service, suivez la procédure relative à l'agent Microsoft SharePoint Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales et cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre Propriétés de Ouvrir une session en tant que service apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Octroi du droit Déboguer les programmes

Vous pouvez accorder le droit Déboguer les programmes.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, suivez la procédure relative à l'agent Microsoft SharePoint Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales et cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre Propriétés de Déboguer les programmes apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Configuration de la surveillance de Microsoft SQL Server

Vous devez configurer l'Monitoring Agent for Microsoft SQL Server pour qu'il puisse collecter des données de l'application surveillée.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft SQL Server.

Vous pouvez installer et configurer l'agent Microsoft SQL Server en local à l'aide de l'interface d'invite de commande. Vérifiez que l'agent est installé sur le serveur surveillé.

Pourquoi et quand exécuter cette tâche

L'agent Microsoft SQL Server est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 139. Versions d'agent et documentation

Version de l'agent Microsoft SQL Server	Documentation
6.3.1.11	IBM Cloud Application Performance Management
6.3.1.9	IBM Performance Management 8.1.3 *
6.3.1.7	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

- Pour configurer l'agent, procédez comme suit :
  - Créez un utilisateur et accordez-lui les droits requis
  - Sélectionnez les bases de données à surveiller
  - Configurez les variables d'environnement local
- Pour exécuter l'agent dans un environnement cluster, procédez comme décrit dans la rubrique «Exécution de l'agent dans un environnement cluster».

Création d'un utilisateur et attribution des droits d'accès

Sur Microsoft SQL Server, vous devez créer un utilisateur sous lequel l'agent sera exécuté, puis octroyer des droits d'accès à l'utilisateur pour la surveillance de Microsoft SQL Server. Le processus d'attribution de droits est identique pour Microsoft SQL Server 2005 et les versions ultérieures.

Avant de commencer

Installez l'agent Microsoft SQL Server. Pour créer un utilisateur et lui octroyer des droits d'accès, vous devez être un administrateur de base de données avec le rôle d'autorisation sysdamin.

Pourquoi et quand exécuter cette tâche

Utilisez la procédure suivante pour déterminer si un utilisateur SQL Server existant dispose de droits suffisants pour surveiller Microsoft SQL Server :

- «Vérification des droits d'un utilisateur SQL Server existant»

Utilisez l'une des procédures suivantes pour créer un utilisateur :

- «Création d'un ID utilisateur SQL Server avec l'authentification Windows», à la page 506
- «Création d'un ID utilisateur SQL Server avec l'authentification SQL Server», à la page 507

Utilisez la procédure suivante pour octroyer des droits :

- «Octroi de droits d'accès minimum pour la collecte de données», à la page 507
- «Octroi d'un droit à la clé de registre Perflib lui permettant de collecter les données de quelques ensembles de données», à la page 509

Vérification des droits d'un utilisateur SQL Server existant

Vous pouvez exécuter l'utilitaire **koqVerifyPerminssions.exe** pour vérifier si un utilisateur SQL Server existant dispose de droits suffisants pour les bases de données SQL Server.

Pourquoi et quand exécuter cette tâche

L'utilitaire **koqVerifyPerminssions.exe** renvoie le message `PASS` si l'utilisateur possède le rôle **sysadmin** ou les droits minimaux requis. Le résultat détaillé de la vérification est consigné dans `koqVerifyPermissions_log`.

Les droits minimaux sont répertoriés ci-dessous :

- Les droits du serveur doivent inclure **Afficher l'état du serveur**, **Afficher une base de données** et **Afficher une définition**.

  Ces droits de niveau serveur sont obligatoires.
- Pour toutes les bases de données système et les bases de données définies par l'utilisateur pour la surveillance, l'appartenance au rôle de base de données doit inclure **public** et **db_owner**.

  Les droits **db_owner** sont requis pour collecter des données des ensembles de données suivants :
  - Ensemble de données des détails du serveur
  - Ensemble de données des détails de la base de données
  - Ensemble de données de la fonction miroir de la base de données
  - Ensemble de données du récapitulatif du serveur
  - Ensemble de données du récapitulatif du journal
- Pour la base de données **msdb**, l'appartenance au rôle de base de données doit inclure **db_datareader**, **SQLAgentReaderRole** et **SQLAgentUserRole**. Ces droits sont requis pour l'ensemble de données Détails du travail.

Procédure

1. Lancez l'invite de commande et accédez au répertoire de l'utilitaire ci-après.
   - Pour les agents 64 bits, *rép_base_agent*\TMAITM6_x64
   - Pour les agents 32 bits, *rép_base_agent* \TMAITM6

   , *rép_base_agent* représentant le répertoire d'installation de l'agent.
2. Exécutez la commande **koqVerifyPerminssions.exe** en spécifiant les paramètres suivants :
   `koqVerifyPermissions.exe -S nom_instance -U nom_utilisateur -P mot_passe`

   Où :
   - *nom_instance* représente le nom de l'instance SQL Server.
   - *nom_utilisateur* représente le nom d'utilisateur vérifié par l'utilitaire.
   - *mot_passe* représente le mot de passe de l'utilisateur. Ce paramètre est requis si *nom_utilisateur* est spécifié.

   Remarque : Si *nom_utilisateur* et *mot_passe* ne sont pas spécifiés, l'utilisateur par défaut connecté au système est utilisé. Exemple : `NT AUTHORITY\SYSTEM`.

Résultats

Le résultat détaillé de la vérification est disponible dans `koqVerifyPermissions_log`, dans le répertoire suivant :

- Pour les agents 64 bits, *rép_base_agent*\TMAITM6_x64\logs
- Pour les agents 32 bits, *rép_base_agent* \TMAITM6\logs

, *rép_base_agent* représentant le répertoire d'installation de l'agent.

Création d'un ID utilisateur SQL Server avec l'authentification Windows

Créez un utilisateur avec l'authentification Windows et affectez-lui les rôles et droits d'accès requis.

Procédure

Pour créer un utilisateur, procédez comme suit :

1. Dans **SQL Server Management Studio**, ouvrez **Object Explorer**.
2. Cliquez sur ***nom_instance_serveur*** > **Sécurité** > **Connexions**.
3. Cliquez avec le bouton droit de la souris sur **Connexions** et sélectionnez **Nouvelle connexion**.
4. Dans la zone **Nom de connexion** de la page **Général**, entrez le nom d'un utilisateur Windows.
5. Sélectionnez **Authentification Windows**.
6. En fonction du rôle et des droits d'accès que vous souhaitez affecter à cet utilisateur, effectuez l'une des tâches suivantes :
   - Dans la page Rôles du serveur, affectez le rôle *sysadmin* au nouvel ID de connexion.
   - Si vous ne souhaitez pas affecter le rôle *sysadmin* à l'utilisateur, octroyez-lui des droits d'accès minimum en effectuant les étapes mentionnées dans la rubrique «Octroi de droits d'accès minimum pour la collecte de données», à la page 507.

   Important : Par défaut, le rôle *public* est affecté au nouvel ID de connexion.
7. Cliquez sur **OK**.

Résultats

Un utilisateur est créé avec le rôle *public* par défaut et les droits d'accès que vous lui avez affectés ; il est affiché dans la liste **Connexions**.

Création d'un ID utilisateur SQL Server avec l'authentification SQL Server

Créez un utilisateur avec l'authentification SQL Server et affectez-lui les rôles et droits d'accès requis.

Procédure

Pour créer un utilisateur, procédez comme suit :

1. Dans **SQL Server Management Studio**, ouvrez **Object Explorer**.
2. Cliquez sur *nom_instance_serveur* > **Sécurité** > **Connexions**.
3. Cliquez avec le bouton droit de la souris sur **Connexions** et sélectionnez **Nouvelle connexion**.
4. Dans la zone **Nom de connexion** de la page **Général**, entrez le nom d'un nouvel utilisateur.
5. Sélectionnez **Authentification SQL Server**.
6. Dans la zone **Mot de passe**, entrez un mot de passe pour l'utilisateur.
7. Dans la zone **Confirmer le mot de passe**, entrez le mot de passe que vous avez saisi dans la zone **Mot de passe** une seconde fois.
8. En fonction du rôle et des droits d'accès que vous souhaitez affecter à cet utilisateur, effectuez l'une des tâches suivantes :
   - Dans la page Rôles du serveur, affectez le rôle *sysadmin* au nouvel ID de connexion.
   - Si vous ne souhaitez pas affecter le rôle *sysadmin* à l'utilisateur, octroyez-lui des droits d'accès minimum en effectuant les étapes mentionnées dans la rubrique «Octroi de droits d'accès minimum pour la collecte de données».

   Important : Par défaut, le rôle *public* est affecté au nouvel ID de connexion.
9. Cliquez sur **OK**.

Résultats

Un utilisateur est créé avec le rôle *public* par défaut et les droits d'accès que vous lui avez affectés ; il est affiché dans la liste **Connexions**.

Octroi de droits d'accès minimum pour la collecte de données

En dehors du rôle **public** par défaut, vous pouvez affecter le rôle **sysadmin** à un utilisateur ou lui octroyer les droits minimaux pour que l'agent puisse collecter des données pour les ensembles de données.

Pourquoi et quand exécuter cette tâche

Vous pouvez octroyer les droits via l'interface utilisateur ou l'utilitaire **permissions.cmd**.

Procédure

- Pour octroyer les droits d'accès minimaux à l'utilisateur via l'interface utilisateur, procédez comme suit :
  1. Ouvrez la page **Rôles du serveur** et vérifiez que la case **public** est cochée.
  2. Ouvrez la page **Mappage de l'utilisateur**, puis cochez les cases suivantes pour toutes les bases de données système et les bases de données définies par l'utilisateur que vous souhaitez surveiller :
     - **public**
     - **db_owner**

     Pour la base de données **msdb**, cochez les cases supplémentaires suivantes :
     - **db_datareader**
     - **SQLAgentReaderRole**
     - **SQLAgentUserRole**

3. Ouvrez la page **Securables**, puis cochez les cases suivantes pour l'instance de serveur que vous surveillez :
   - view database
   - view definition
   - view server state

- Pour octroyer les droits d'accès minimaux à l'utilisateur à l'aide de l'utilitaire **permissions.cmd**, procédez comme suit :
  1. Lancez Windows Explorer et accédez au répertoire *rép_octroi_droits_agent* de l'utilitaire :
     - Pour l'agent 64 bits, *rép_octroi_droits_agent* correspond à *rép_base_agent*\TMAITM6_x64\scripts\KOQ\GrantPermission.
     - Pour l'agent 32 bits, *rép_octroi_droits_agent* correspond à *rép_base_agent*\TMAITM6\scripts\KOQ\GrantPermission.
     - *rép_base_agent* représente le répertoire d'installation de l'agent.

     Avertissement : L'utilitaire **permissions.cmd** octroie les droits **db_owner** sur toutes les bases de données par défaut. Pour exclure certaines bases de données, vous devez ajouter les noms de base de données dans le fichier *rép_octroi_droits_agent*\exclude_database.txt. Les noms de base de données doivent être séparés par le symbole alias **@**.

     Conseil : Par exemple, si vous souhaitez exclure les bases de données **MyDatabase1** et **MyDatabase2**, ajoutez l'entrée suivante dans le fichier exclude_database.txt :

     ```
     MyDatabase1@MyDatabase2
     ```
  2. Cliquez deux fois sur **permissions.cmd** pour lancer l'utilitaire.
  3. Entrez les valeurs de paramètre prévues lorsque vous y êtes invité :

Tableau 140. Paramètres

Paramètres	Description
Nom SQL Server ou nom d'instance SQL Server	Entrez le nom SQL Server cible ou le nom d'instance SQL Server cible qui doit octroyer les droits à l'utilisateur.
Nom de connexion de l'utilisateur SQL Server existant	Entrez le nom d'utilisateur dont les droits seront modifiés.
Options de droits : **1** Octroie les droits **db_owner** **2** Octroie les droits **db_datareader**, **SQLAgentReaderRole** et **SQLAgentUserRole** **3** Octroie tous les droits requis	Entrez **1**, **2** ou **3** selon vos besoins.
Utilisateur auquel les droits doivent être octroyés : **1** Utilisateur actuellement connecté au système **2** Autre utilisateur	Entrez **1** ou **2**. Si **2** est sélectionné, entrez le nom d'utilisateur cible lorsque vous y êtes invité. **Remarque :** Les utilisateurs doivent avoir accès pour octroyer des droits à d'autres utilisateurs.

Que faire ensuite

Configurez l'agent.

Octroi d'un droit à la clé de registre Perflib lui permettant de collecter les données de quelques ensembles de données

Pour collecter les données de quelques ensembles de données, vous devez accorder aux utilisateurs un accès en lecture à la clé de registre Perflib.

Pourquoi et quand exécuter cette tâche

Vous devez accorder ce droit à l'utilisateur Windows avec lequel les services d'agent sont configurés. Un grand nombre d'ensembles de données sont affectés en l'absence de droits Perflib, tels que MS SQL Database Detail, MS SQL Memory Manager, MS SQL Lock Resource Type Summary, MS SQL Job Summary, MS SQL Server Transactions Summary, MS SQL Server Summary, etc.

Procédure

Pour accorder ce droit à la clé de registre Perflib, procédez comme suit :

1. Pour ouvrir l'éditeur de registre, cliquez sur **Démarrer** > **Exécuter** > **Regedit.exe**, et appuyez sur **Entrée**.
2. Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.
3. Cliquez avec le bouton droit de la souris sur la clé **Perflib**, puis cliquez sur **Droits**.
4. Cliquez sur **Ajouter**, entrez le nom de l'utilisateur Windows avec lequel l'agent est installé et configuré, puis cliquez sur **OK**.
5. Cliquez sur l'utilisateur que vous avez ajouté.
6. Accordez à l'utilisateur un accès en lecture en cochant la case correspondante.
7. Cliquez sur **Appliquer**, puis sur **OK**.

Exécution en tant qu'utilisateur non-administrateur

Vous pouvez exécuter l'agent de surveillance pour Microsoft SQL Server en tant qu'utilisateur non-administrateur.

Pourquoi et quand exécuter cette tâche

agent Microsoft SQL Server peut être exécuté en tant qu'utilisateur non-administrateur. Dans ce cas, seuls les utilisateurs de domaine sont pris en charge.

Procédure

1. Démarrez l'application Windows Utilisateurs et ordinateurs Active Directory et créez un utilisateur de domaine.
   - Vérifiez que le nouvel utilisateur fait bien partie du groupe *Utilisateurs du domaine*.
   - Vérifiez que le serveur SQL Server que vous surveillez fait bien partie du groupe *Ordinateurs du domaine*.
2. Ajoutez l'utilisateur de domaine que vous venez de créer au groupe d'utilisateurs *Connexion à SQL Server*. L'utilisateur de domaine doit disposer soit des droits du rôle SQL Server sysadmin sur le serveur SQL Server, soit des droits indiqués dans https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/sql_config_agent_grant_permission_sqlserver.htm.
3. Connectez-vous au serveur SQL Server à l'aide d'un compte d'administrateur de domaine.
4. Utilisez les **Systèmes de fichiers** pour accorder le droit de modification sur chaque unité à laquelle l'agent Microsoft SQL Server a accès et propager les droits à tous les sous-répertoires. Procédez comme suit pour propager les droits :
   a. Allez dans **Poste de travail**.
   b. Cliquez avec le bouton droit de la souris sur l'**unité**.

c. Cliquez sur l'onglet **Sécurité**.
d. Ajoutez le nouvel utilisateur.
e. Accordez les droits de modification à l'utilisateur qui vient d'être créé.
f. Cliquez sur **OK**. L'application des droits sur tout le système de fichiers prend quelques minutes.

5. A partir du registre Windows, accordez un accès en lecture à `HKEY_LOCAL_MACHINE` et propagez les paramètres. Procédez comme suit pour propager les paramètres :
   a. Cliquez avec le bouton droit de la souris sur le répertoire `HKEY_LOCAL_MACHINE` et sélectionnez **Droits**.
   b. Ajoutez le nouvel utilisateur.
   c. Sélectionnez le nouvel utilisateur.
   d. Cochez la case **Autoriser la lecture**.
   e. Cliquez sur **OK**. La propagation des droits à toute l'arborescence de `HKEY_LOCAL_MACHINE` prend quelques minutes.
6. A partir du Registre Windows, accordez des droits sur le Registre spécifiques à l'agent en fonction de la liste suivante.
   - Si vous avez installé un agent 32 bits sur un système d'exploitation 32 bits, accordez un accès complet au répertoire `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` et propagez les paramètres.
   - Si vous avez installé un agent 32 bits sur un système d'exploitation 64 bits, accordez un accès complet au répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Candle` et propagez les paramètres.
   - Si vous avez installé un agent 64 bits sur un système d'exploitation 64 bits, accordez un accès complet au répertoire `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` et propagez les paramètres.

   Procédez comme suit pour propager les paramètres :
   a. Cliquez avec le bouton droit de la souris sur le répertoire pour lequel vous disposez d'un accès complet et sélectionnez **Droits**.
   b. Ajoutez le nouvel utilisateur.
   c. Sélectionnez l'utilisateur qui vient d'être créé.
   d. Cochez la case **Autoriser le plein contrôle**.
   e. Cliquez sur **OK**. La propagation des droits à toute l'arborescence de `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` prend quelques minutes.
7. Ajoutez un nouvel utilisateur de domaine au groupe *Utilisateurs de l'Analyseur de performances*.
8. Vérifiez que le groupe Utilisateurs de domaine fait partie du groupe *Utilisateurs*.
9. Accordez les droits suivants sur le répertoire Windows pour une exécution en tant qu'utilisateur non-administrateur :
   - Si un agent 32 bits est installé sur un système d'exploitation 32 bits, accordez un accès en lecture et en écriture au répertoire `unité_installation_SE:\Windows\system32`
   - Si un agent 32 bits est installé sur un système d'exploitation 64 bits, accordez un accès en lecture et en écriture au répertoire `unité_installation_SE:\Windows\SysWOW64`

   Remarque : Des droits sur le répertoire Windows ne sont pas nécessaires pour Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 et Windows Server 2016.
10. Accordez le droit de modification sur le fichier de données SQL Server et sur le fichier journal :
    - Le chemin par défaut du fichier de données est *rép_principal_SQLServer*`\DATA`, où *rép_principal_SQLServer* représente le répertoire principal de l'instance SQL Server. Par exemple, si le répertoire principal de l'instance SQL Server est `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL`, le chemin du fichier de données sera `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA`.

- Le chemin par défaut du fichier journal est *rép_principal_SQLServer*\LOG, où *rép_principal_SQLServer* représente le répertoire principal de l'instance SQL Server. Par exemple, si le répertoire principal de l'instance SQL Server est C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL, le chemin du fichier journal sera C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG.

11. Accordez un accès complet au répertoire rép_principal_candle. Le chemin par défaut est C:\IBM\ITM.
12. Appliquez les droits de sécurité locaux (voir «Droits de la stratégie de sécurité locale»).
13. Redémarrez SQL Server pour vous assurer que les droits de sécurité locaux sont bien appliqués.
14. Modifiez les paramètres de connexion de l'utilisateur non-administrateur pour les services d'agent SQL Server. Pour ce faire, procédez comme suit :
    a. Cliquez sur **Démarrer > Outils d'administration > Services**.
    b. Cliquez avec le bouton droit de la souris sur le service **Agent de surveillance pour SQL Server *nom_instance***, puis cliquez sur **Propriétés**. La fenêtre Propriétés de Service SQL s'affiche.
    c. Cliquez sur l'onglet **Connexion**.
    d. Cliquez sur **Ce compte** et entrez le nom de l'utilisateur.
    e. Dans les zones **Mot de passe** et **Confirmer le mot de passe**, entrez le mot de passe et cliquez sur **OK**.
    f. Répétez les étapes b à e pour l'**Agent de surveillance du collecteur SQL Server *nom_instance***, où *nom_instance* représente le nom d'instance de Microsoft SQL Server.

Droits de la stratégie de sécurité locale

La stratégie de sécurité locale administre le système et ses règles de sécurité. Elle joue un rôle important dans le maintien de la sécurité de l'agent et du système sur lequel l'agent est installé. Cette stratégie fonctionne en donnant des droits et des droits aux utilisateurs. Dans le cas de l'agent Microsoft SQL Server, assurez-vous que l'utilisateur dispose les droits suivants afin de respecter les règles de la stratégie de sécurité locale.

Droit Ouvrir une session en tant que service :

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Ouvrir une session en tant que service, suivez la procédure relative à l'agent Microsoft SQL Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre Propriétés de Ouvrir une session en tant que service apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Droit Déboguer les programmes :

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, suivez la procédure relative à l'agent Microsoft SQL Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre Propriétés de Déboguer les programmes apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Simuler les droits d'un client après l'authentification :

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Simuler les droits d'un client après l'authentification, suivez la procédure relative à l'agent Microsoft SQL Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Simuler les droits d'un client après l'authentification**. La fenêtre Propriétés de Simuler les droits d'un client après l'authentification apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Sélection des bases de données à surveiller

Vous pouvez sélectionner la base de données à surveiller en utilisant la fenêtre Configure Database Agents.

Procédure

1. Ouvrez la fenêtre IBM Performance Management.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne Tâche/sous-système, puis sélectionnez **Configurer avec les valeurs par défaut**.
3. Dans la fenêtre Configure Database Agents, sélectionnez le serveur de base de données à surveiller dans la liste **Database Servers Available**, puis cliquez sur la flèche gauche pour déplacer le serveur vers la liste **Server to Monitor**.

4. Dans la fenêtre Propriétés du serveur de base de données, les valeurs des zones suivantes sont automatiquement indiquées :
   - nom de serveur
   - Database Version
   - Home Directory
   - Error Log File

   Les zones suivantes de la fenêtre Propriétés du serveur de base de données sont facultatives :
   - Windows Authentication
   - Support Long Lived Database Connections
   - Extended Parms
   - Monitor all Databases
   - Day(s) Frequency
   - Weekly Frequency
   - Monthly Frequency
   - Collection Start Time
   - Table Detail Continuous Collection

   Pour plus d'informations sur les paramètres de configuration de la fenêtre Propriétés du serveur de base de données, voir «Paramètres de configuration des propriétés du serveur de base de données», à la page 514.
5. Si vous ne sélectionnez pas la zone **Authentification Windows**, entrez votre ID utilisateur et votre mot de passe dans les zones **Login** et **Password** en utilisant uniquement des caractères ASCII.
6. Dans la zone **Extended Parms**, entrez le nom de l'un des ensembles de données pour désactiver la collecte des données, puis cliquez sur **OK**.

   Par exemple :
   - `koqtbld` pour l'ensemble de données Table Detail
   - `koqdbd` pour l'ensemble de données Détails des bases de données
   - `koqtbld,koqdbd` pour désactiver l'ensemble de données Détails de la table et Détail des bases de données
7. Si vous ne cochez pas la case **Surveillance de toutes les bases de données**, vous devez indiquer la liste de bases de données pour lesquelles vous souhaitez activer ou désactiver la surveillance dans la zone de texte de la zone de groupe **Bases de données**.

   A faire : Si vous cochez la case **Surveillance de toutes les bases de données** et indiquez les bases de données à surveiller dans la zone de texte située dans la zone de groupe **Bases de données**, la priorité est donnée à la valeur de la case **Surveillance de toutes les bases de données**. La liste des bases de données que vous indiquez dans la zone de texte est ignorée.
8. Définissez une fréquence quotidienne, hebdomadaire ou mensuelle pour la collecte de l'ensemble de données MS SQL Table Detail.
9. Cochez la case **Table Detail Continuous Collection** pour activer la collecte continue de l'ensemble de données MS SQL Table Detail. Si vous cochez la case **Table Detail Continuous Collection**, entrez une valeur dans la zone **Interval Between Two Continuous Collection (in minutes)**.
10. Dans la fenêtre Configure Database Agents, cliquez sur **OK**, puis démarrez l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration des propriétés du serveur de base de données

Dans la fenêtre des propriétés du serveur de base de données, vous pouvez configurer des propriétés du serveur de base de données, telles que le nom du serveur, la version de base de données et le répertoire de base.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de la fenêtre des propriétés du serveur de base de données.

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données

Nom du paramètre	Description	Zone obligatoire	Exemples
nom de serveur	Nom de l'instance Microsoft SQL Server à surveiller. Utilisez MSSQLSERVER comme nom d'instance de l'instance par défaut. Le nom doit être suffisamment court pour répondre aux exigences des noms de système géré qui admettent de 2 à 32 caractères.	Oui	Si l'instance Microsoft SQL Server surveillée est l'instance Microsoft SQL Server par défaut, entrez `MSSQLSERVER` dans cette zone. Si l'instance Microsoft SQL Server surveillée est une instance nommée (où le nom de l'instance est `mysqlserver` et le nom d'hôte est `popcorn`), entrez `mysqlserver` dans cette zone.
Connexion	ID utilisateur Microsoft SQL Server à utiliser pour se connecter à Microsoft SQL Server. L'ID utilisateur n'est obligatoire que si le paramètre **`Windows Authentication`** est défini sur `False`. Utilisez uniquement des caractères ASCII pour l'ID utilisateur. Lorsque vous configurez l'agent Microsoft SQL Server en indiquant un ID de connexion dans la zone **Connexion**, l'agent utilise cet ID pour se connecter à Microsoft SQL Server. **Important :** Si, lors de la configuration de l'agent, vous sélectionnez la case à cocher **Authentification Windows** et que vous indiquez un ID de connexion dans la zone **Connexion**, l'agent donne la préférence à l'authentification Windows.	Non	
mot de passe	Mot de passe associé à l'ID utilisateur Microsoft SQL Server. Le mot de passe n'est obligatoire que si le paramètre **`Windows Authentication`** est défini sur `False`. Utilisez uniquement des caractères ASCII pour le mot de passe.	Non	

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
Version de la base de données	Version de l'instance SQL Server.	Oui	Les versions de base de données de l'instance SQL Server sont les suivantes : • Microsoft SQL Server 2014 - 12.0.2000.8 • Microsoft SQL Server 2012 - 11.0.2100.60 • Microsoft SQL Server 2008 R2 - 10.50.1600.1 • Microsoft SQL Server 2008 - 10.0.1600.22 • Microsoft SQL Server 2005 - 9.0.1399.06
Répertoire de base	Répertoire d'installation de SQL Server.	Oui	Le chemin d'accès par défaut au répertoire de base pour l'instance Microsoft SQL Server 2005 est `C:\Program Files\Microsoft SQL Server\MSSQL`. Une instance Microsoft SQL Server 2005 nommée dispose d'un chemin d'accès par défaut au répertoire de base au format `C:\Program Files\Microsoft SQL Server\MSSQL$`*`nom_instance`*, où *nom_instance* est le nom de l'instance Microsoft SQL Server.

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
Fichier journal des erreurs	Emplacement et nom qualifiés complets du journal des erreurs SQL Server.	Oui	Le chemin d'accès par défaut au journal des erreurs de l'instance Microsoft SQL Server 2005 par défaut est `C:\Program Files\Microsoft SQL Server\MSSQL\LOG\ ERRORLOG`. Une instance Microsoft SQL Server 2005 nommée dispose d'un chemin d'accès par défaut au journal des erreurs au format `C:\Program Files\Microsoft SQL Server\ MSSQL$`*`nom_instance`*`\LOG\ ERRORLOG`, où *nom_instance* est le nom de l'instance Microsoft SQL Server.

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
Authentification Windows	L'authentification Windows est un compte Windows sous lequel les services d'agent sont configurés. Il s'agit de l'option de configuration par défaut. Si vous sélectionnez la case à cocher **Windows**, les informations d'identification Windows sont utilisées pour l'authentification. Lorsque l'agent Microsoft SQL Server est configuré avec l'authentification Windows, le **Compte système local** ou **Ce compte** est utilisé par les services d'agent pour la connexion à Microsoft SQL Server. • Si les services d'agent sont configurés pour utiliser le **Compte système local** pour se connecter, alors l'agent utilise l'ID utilisateur NT AUTHORITY\SYSTEM pour accéder à Microsoft SQL Server. • Si les services d'agent sont configurés pour utiliser **Ce compte** pour se connecter, alors l'agent utilise l'ID utilisateur respectif pour accéder à Microsoft SQL Server. **A faire :** Si vous ne sélectionnez pas la case à cocher **Authentification Windows**, vous devez indiquer des valeurs pour les paramètres **Connexion** et **Mot de passe**. Si vous n'indiquez pas ces paramètres et que vous cliquez sur **OK** dans la fenêtre Propriétés du serveur de base de données, un message d'erreur s'affiche dans une fenêtre en incrustation et la configuration de l'agent n'aboutit pas. **Important :** Si, lors de la configuration de l'agent, vous sélectionnez la case à cocher **Authentification Windows** et que vous indiquez un ID de connexion dans la zone **Connexion**, l'agent donne la préférence à l'authentification Windows.	Non	
Prise en charge des connexions de base de données de longue durée	Active ou désactive les connexions de base de données de longue durée. Les connexions de base de données de longue durée ne sont pas utilisées dans les ensembles de données suivants : • Texte MS SQL • Détail des groupes de fichiers MS SQL • Récapitulatif Microsoft SQL Server	Non	

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
Paramètres étendus	Désactive la collecte de données de n'importe quel groupe d'attributs.	Non	Par exemple : Pour désactiver la collecte de données pour l'ensemble de données Détail des tables, entrez `koqtbld` dans la zone **Extended Parms**. Pour désactiver la collecte de données pour l'ensemble de données Détail des bases de données, entrez `koqdbd` dans la zone **Extended Parms**. Pour désactiver la collecte de données pour les ensembles de données Table Details et Database Details, entrez `koqtbld,koqdbd` dans la zone **Extended Parms**.

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples

Base de données	Pour sélectionner les bases de données à surveiller, indiquez une valeur pour ce paramètre. Pour activer la surveillance de toutes les bases de données disponibles dans l'instance de serveur SQL, cochez la case **Surveillance de toutes les bases de données** dans le groupe **Bases de données**.
	
	Conseil : La case **Surveillance de toutes les bases de données** est sélectionnée par défaut.
	
	Pour activer ou désactiver la surveillance de bases de données spécifiques, désélectionnez la case **Surveillance de toutes les bases de données**.
	• Pour surveiller des bases de données spécifiques, sélectionnez **Include** dans la liste, puis indiquez les noms des bases de données dans la zone de texte en regard de la liste.
	• Pour exclure des bases de données spécifiques de la surveillance, sélectionnez **Exclude** dans la liste, puis indiquez les noms des bases de données dans la zone de texte en regard de la liste.
	
	Utilisez cette zone de texte pour filtrer les bases de données que vous voulez surveiller.
	
	Pour indiquer le filtre de bases de données, vous devez d'abord sélectionner un séparateur. Un séparateur est un caractère qui distingue un nom de base de données ou une expression de base de données d'un autre nom de base de données ou d'une autre expression de base de données. Lorsque vous sélectionnez un séparateur, vérifiez que les noms de base de données et l'expression de base de données ne contiennent pas le caractère que vous choisissez comme séparateur. Vous ne devez pas utiliser les caractères génériques généralement utilisés dans la requête T-SQL (par exemple : %, _, [ ], ^, -) s'ils sont utilisés dans les noms de base de données ou dans l'expression de base de données.
	
	Lorsque vous spécifiez un filtre de base de données :
	• Les noms de base de données doivent commencer par un séparateur.
	• L'expression de base de données doit commencer par deux séparateurs.
	
	Remarque : L'expression de base de données est une expression valide qui peut être utilisée dans la section `LIKE` de la requête `T-SQL`. Toutefois, la clause `T-SQL ESCAPE` n'est pas autorisée lorsque vous spécifiez l'expression de base de données. Un filtre de base de données affecte les ensembles de données suivants :
	• Détail des bases de données
	• Récapitulatif de la base de données
	• Détail des unités
	• Détail des tables
		Non	Exemples de filtres :
			
			Cas 1 : `% d'utilisation`
			
			Exemple :
			`@@%m%`
			
			Résultat : toutes les bases de données ayant le caractère m dans leur nom sont filtrées.
			
			Cas 2 : `utilisation de _`
			
			Exemple :
			`@@____`
			
			Résultat : toutes les bases de données d'une longueur de quatre caractères sont filtrées.
			
			Cas 3 : `utilisation de []`
			
			Exemple :
			`@@[m]___`
			
			Résultat : toutes les bases de données d'une longueur de quatre caractères et dont le nom commence par le caractère m sont filtrées.
			
			Cas 4 : `utilisation de [^]`
			
			Exemple :
			`@@[^m]%`
			
			Résultat : toutes les bases de données (quelle que soit leur longueur) exceptées celles dont le nom commence par le caractère *m* sont filtrées.

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples

Database (suite)	**A faire :**
	• Si vous ne cochez pas la case **Surveillance de toutes les bases de données**, vous devez indiquer la liste de bases de données pour lesquelles vous souhaitez activer ou désactiver la surveillance dans la zone de texte figurant dans le groupe **Bases de données**. Si vous cliquez sur **OK** dans la fenêtre Propriétés du serveur de base de données sans cocher la case **Surveillance de toutes les bases de données** et indiquer la liste de bases de données, un message d'erreur s'affiche dans une fenêtre en incrustation et la configuration de l'agent n'aboutit pas.
	• Si vous cochez la case **Surveillance de toutes les bases de données** et indiquez les bases de données à surveiller dans la zone de texte située dans le groupe **Bases de données**, la priorité est donnée à la valeur de la case **Surveillance de toutes les bases de données**. La liste de bases de données indiquée dans la zone de texte est ignorée.
			Cas 5 : entrée erronée
			Exemple :
			`@%m%`
			Résultat : aucune des bases de données n'est filtrée.
			Cas 6 : option par défaut
			Exemple : zone laissée vide (aucune requête n'est saisie)
			Résultat : toutes les bases de données sont filtrées.
			Cas 7 : modèles mixtes
			Exemple :
			`@@[m-t]_d%`
			Résultat : toutes les bases de données (quelle que soit leur longueur) dont le noms commence par le caractères m, n, o, p, q, r, s, t, suivi d'un caractère quelconque, avec le caractère d en troisième position, sont filtrées.

Day(s) Frequency	Utilisez cette fonction pour définir la fréquence de collecte des données des attributs Détail des tables. Les valeurs sont comprises entre zéro et 31.	Non	
Weekly Frequency	Utilisez cette fonction pour définir un jour particulier pour la collecte des données des attributs Détail des tables. Les valeurs sont comprises entre zéro et sept.	Non	
Monthly Frequency	Utilisez cette fonction pour définir la fréquence de collecte des données des attributs Détail des tables sur un jour donné du mois. Les valeurs possibles sont 1, 2, 3, etc.	Non	
Collection Start Time	Heure de début de la collecte au format HH:MM. Les valeurs possibles pour les heures vont de zéro à 23. La valeur par défaut est zéro. Les valeurs possibles pour les minutes vont de zéro à 59. La valeur par défaut est zéro.	Non	

Tableau 141. Noms et descriptions des paramètres de configuration de la fenêtre des propriétés du serveur de base de données (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
Table Detail Continuous Collection	Utilisez cette fonction pour collecter en arrière-plan de manière continue les données de détail des tables. La case **Table Detail Continuous Collection** est cochée par défaut.	Non	
Interval Between Two Continuous Collection (in min.)	Durée de l'intervalle entre deux collectes en minutes. L'intervalle minimum est de 3 minutes. Vous pouvez cocher la case **Interval Between Two Continuous Collection (in min.)** ou utiliser la planification pour spécifier la collecte continue de l'ensemble de données Détail des tables. Si vous cochez la case **Interval Between Two Continuous Collection (in min.)**, vous devez spécifiez l'intervalle de temps pour la collection. Si vous utilisez la planification pour spécifier la collecte de l'ensemble de données Détail des tables, l'intervalle de temps minimal est de 1 jour. L'intervalle par défaut entre deux collectes continues est de 3 minutes.	Non	

L'agent collecte les données à l'intervalle de temps où la collecte de données se produit fréquemment. Par exemple, si vous spécifiez toutes les fréquences (quotidienne, hebdomadaire et mensuelle) pour la collecte des données, l'agent démarre la collecte des données en tenant compte des critères suivants :

- Si la fréquence quotidienne est ≤ 7, les paramètres de fréquence quotidienne sont sélectionnés et les paramètres de fréquence hebdomadaire et mensuelle sont ignorés.
- Si la fréquence quotidienne est > 7, les paramètres de fréquence hebdomadaire sont sélectionnés et les paramètres de fréquence quotidienne et mensuelle sont ignorés.

A faire : Si la case **Table Detail Continuous Collection** est cochée, l'agent collecte les données à l'intervalle défini par la zone **Interval Between Two Continuous Collection (in min.)** et non selon les fréquences quotidienne, hebdomadaire ou mensuelle.

Définition des variables d'environnement local

Vous pouvez définir les variables d'environnement local pour modifier le comportement de agent Microsoft SQL Server.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, dans le menu **Actions**, cliquez sur **Advanced > Editer les variables**.
3. Dans la fenêtre Monitoring Agent for Microsoft SQL Server: Override Local Variable Settings, cliquez sur **Ajouter**.
4. Dans la fenêtre Ajouter la substitution des paramètres d'environnement, entrez la variable et la valeur correspondante.

   Pour afficher la liste des variables d'environnement que vous pouvez configurer, voir «Variables d'environnement local», à la page 522.

Variables d'environnement local

Vous pouvez changer le comportement de agent Microsoft SQL Server en définissant les variables d'environnement local.

Variables de vérification de disponibilité du service SQL Server

Pour vérifier la disponibilité du service SQL Server, ajoutez les variables d'environnement suivantes :

- **COLL_MSSQL_RETRY_INTERVAL** : cette variable définit l'intervalle entre deux tentatives (en minutes) de vérification du statut du service SQL Server. Si la valeur est inférieure ou égale à zéro, la variable utilise la valeur par défaut 1 minute.
- **COLL_MSSQL_RETRY_CNT** : cette variable définit le nombre de tentatives de l'agent SQL pour vérifier que le service SQL Server est démarré. Si le service SQL Server n'est pas démarré après le nombre de tentatives spécifié dans cette variable, le collecteur s'arrête. Si la valeur de la variable est inférieure ou égale à zéro, la variable utilise la valeur par défaut 3.

Variables de surveillance du fichier journal des événements SQL Server

Pour surveiller l'ensemble de données MS SQL Error Event Details, utilisez les variables d'environnement suivantes :

- **COLL_ERRORLOG_STARTUP_MAX_TIME** : cette variable définit l'intervalle de temps (T) de la collecte des erreurs avant le démarrage de l'agent. La valeur par défaut est `0` minutes. Cette variable peut avoir les valeurs suivantes :

  T = 0 L'agent démarre la surveillance du fichier journal des erreurs lorsqu'il démarre ou redémarre. L'agent ne lit pas les erreurs consignées dans le fichier journal des erreurs avant son démarrage.

  T = 1 L'agent surveille le fichier journal des erreurs en fonction des valeurs suivantes définies pour la variable **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW** représentée par R :
  - Si R < 0, l'agent démarre la surveillance du fichier journal des erreurs lorsqu'il démarre ou redémarre.
  - Si R = 1, l'agent surveille toutes les erreurs consignées dans le fichier journal des erreurs.
  - Si R > 1 et que l'agent est installé pour la première fois, l'agent surveille le fichier journal des erreurs tant les erreurs R sont surveillées. Si R > 1 et que l'agent est redémarré, l'agent surveille toutes les erreurs R manquées.

  T > 1 L'agent surveille toutes les erreurs précédentes consignées jusqu'au nombre de minutes T à partir de son démarrage ou redémarrage. L'agent qui surveille dépend également des valeurs suivantes que vous définissez pour la variable **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW** :
  - Si R ≤ 0, l'agent démarre la surveillance du fichier journal des erreurs lorsqu'il démarre ou redémarre.
  - Si R = 1, l'agent surveille toutes les erreurs consignées dans le fichier journal jusqu'à T minutes.
  - Si R > 1, l'agent ne surveille pas plus de R erreurs consignées au cours des T dernières minutes.
- **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW** : cette variable définit le nombre maximum d'erreurs devant être traitées au démarrage de l'agent. La valeur par défaut est `0`. Vous pouvez affecter les valeurs suivantes à la variable :

  R = 0 L'agent démarre la surveillance du fichier journal des erreurs, dès qu'il démarre ou qu'il redémarre. Il ne lit pas les erreurs qui ont été créées dans le fichier journal des erreurs avant son démarrage.

  R = 1 L'agent surveille les erreurs consignées au cours des T dernières minutes depuis son démarrage ou redémarrage.

R > 1 L'agent surveille les erreurs R consignée au cours des T dernières minutes.

- **COLL_ERRORLOG_MAX_EVENT_ROW** : cette variable fournit le nombre de lignes d'erreur. La valeur par défaut est 50. Vous pouvez affecter les valeurs suivantes à la variable :

  X = 0 L'agent n'affiche pas les journaux d'erreur.

  X > 0 L'agent affiche x lignes d'erreur.
- **COLL_ERRORLOG_RECYCLE_WAIT** : cette variable indique l'intervalle de temps (en secondes) pendant lequel l'agent Microsoft SQL Server attend de collecter les données du groupe d'attributs MS SQL Error Event Detail lorsque la situation de ce groupe d'attributs est déclenchée. Attribuez une valeur comprise entre 1 et 30 à cette variable. Si sa valeur est inférieure à 0, la variable utilise la valeur par défaut 0 (seconde). Si sa valeur est supérieure à 30, la variable utilise la valeur par défaut 30 (secondes).

Variable de définition du délai d'expiration de la requête

Pour définir l'intervalle du délai d'attente de requête pour l'agent SQL Server, utilisez les variables d'environnement suivantes :

- **QUERY_TIMEOUT** : cette variable d'environnement définit le délai maximum (en secondes) pendant lequel SQL Server attend une réponse pour une requête envoyée à SQL Server. La valeur par défaut de cette variable doit être inférieure à 45 secondes. Cependant, si vous définissez la valeur 0 pour cette variable, l'agent SQL Server attend indéfiniment une réponse de SQL Server. Si l'agent SQL Server accède à un grand nombre de bases de données verrouillées, vous devez affecter à cette variable une valeur comprise entre 10 et 20 secondes. Si la requête n'est pas traitée pendant le délai défini, l'agent SQL Server ignore la requête expiré et passe à la requête suivante dans la file d'attente. L'agent n'affiche pas de données pour la requête qui a expiré.
- **QUERY_THREAD_TIMEOUT** : cette variable d'environnement définit le délai maximum (en secondes) pendant lequel SQL Server attend une réponse pour une requête envoyée à SQL Server. Cette variable d'environnement est applicable à quelques groupes d'attributs qui utilisent la collecte basée sur les unités d'exécution. Par exemple, KOQDBD, KOQTBLD, KOQDEVD, etc. La valeur de cette variable n'a aucune limite, contrairement à la variable QUERY_TIMEOUT. Sinon, elle fonctionne de la même manière que la variable QUERY_TIMEOUT.

Variable d'affichage des informations sur les travaux activés

Pour afficher les informations relatives aux travaux activé dans l'ensemble de données MS SQL Job Detail, utilisez la variable d'environnement **COLL_JOB_DISABLED**. Si vous affectez à cette variable la valeur 1, agent Microsoft SQL Server n'affiche pas les informations relatives aux travaux activés. Si vous ne spécifiez pas cette variable, vous pouvez afficher les informations relatives aux travaux activés et désactivés.

Variable permettant de limiter le nombre de lignes dans l'ensemble de données Détail des groupes de fichiers MS SQL

Pour limiter le nombre de lignes extraites par le service de collecteur pour l'ensemble de données Détail des groupes de fichiers MS SQL, utilisez la variable d'environnement **COLL_KOQFGRPD_MAX_ROW**. Cette variable d'environnement définit le nombre maximal de lignes que le service de collecteur extrait pour l'ensemble de données Détail des groupes de fichiers. Si vous n'indiquez pas de valeur pour cette variable, le service de collecteur extrait 10000 lignes pour l'ensemble de données Détail des groupes de fichiers. Utilisez cette variable d'environnement pour modifier le nombre maximal de lignes par défaut dans le fichier koqcoll.ctl. Pour modifier le nombre maximal de lignes par défaut, procédez comme suit :

1. Indiquez le nombre maximal de lignes pour KOQFGRPD dans le fichier koqcoll.ctl.
2. Ajoutez la variable d'environnement **COLL_KOQFGRPD_MAX_ROW** et assurez-vous que la valeur de cette variable est identique à la valeur indiquée dans le fichier koqcoll.ctl.

Si la valeur du fichier koqcoll.ctl est inférieure à la valeur indiquée par la variable d'environnement **COLL_KOQFGRPD_MAX_ROW**, la valeur définie dans le fichier koqcoll.ctl est considérée comme la valeur représentant le nombre maximal de lignes.

Si la valeur du fichier koqcoll.ctl est supérieure à la valeur indiquée dans la variable d'environnement **COLL_KOQFGRPD_MAX_ROW**, la valeur de la variable d'environnement **COLL_KOQFGRPD_MAX_ROW** est considérée comme la valeur représentant le nombre maximal de lignes.

Variables d'optimisation de la collecte de l'ensemble de données Détail des groupes de fichiers MS SQL

Utilisez la variable **COLL_DBD_FRENAME_RETRY_CNT** pour indiquer le nombre de tentatives qui peuvent être effectuées pour déplacer le fichier %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__FGRP_TEMP vers le fichier %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__FGRP_PREV.

Si vous n'indiquez pas de valeur pour cette variable, l'agent Microsoft SQL Server fait trois tentatives de déplacement du fichier.

Variable permettant de limiter le nombre de lignes dans l'ensemble de données MS SQL Device Detail

Pour limiter le nombre de lignes extraites pour le service de collecteur de l'ensemble de données MS SQL Device Detail, utilisez la variable d'environnement **COLL_KOQDEVD_MAX_ROW**. Cette variable d'environnement définit le nombre maximal de lignes que le service de collecteur extrait pour l'ensemble de données Device Detail. Si vous n'indiquez pas de valeur pour cette variable, le service de collecteur extrait 10000 lignes pour l'ensemble de données Device Detail. Utilisez cette variable d'environnement pour modifier le nombre maximal de lignes par défaut dans le fichier koqcoll.ctl. Pour modifier le nombre maximal de lignes par défaut, procédez comme suit :

1. Indiquez le nombre maximal de lignes pour KOQDEVD dans le fichier koqcoll.ctl.
2. Ajoutez la variable d'environnement **COLL_KOQDEVD_MAX_ROW** et vérifiez que la valeur de cette variable est identique à celle indiquée dans le fichier koqcoll.ctl.

Si la valeur du fichier koqcoll.ctl est inférieure à la valeur indiquée par la variable d'environnement **COLL_KOQDEVD_MAX_ROW**, la valeur définie dans le fichier koqcoll.ctl est considérée comme la valeur représentant le nombre maximal de lignes.

Si la valeur du fichier koqcoll.ctl est supérieure à la valeur définie dans la variable d'environnement **COLL_KOQDEVD_MAX_ROW**, la valeur de la variable d'environnement **COLL_KOQDEVD_MAX_ROW** est considérée comme la valeur représentant le nombre maximal de lignes.

Variables d'optimisation de la collecte pour l'ensemble de données MS SQL Device Detail

Pour optimiser la collecte de l'ensemble de données MS SQL Device Detail, utilisez les variables d'environnement suivantes :

- **COLL_KOQDEVD_INTERVAL** : cette variable d'environnement permet d'indiquer un intervalle (en minutes) entre deux collectes consécutives de l'ensemble de données MS SQL Device Detail.

  Remarque : Par défaut, la collecte des données de l'ensemble de données Device Detail est lancée sur demande. Utilisez la variable **COLL_KOQDEVD_INTERVAL** pour démarrer une collecte basée sur des unités d'exécution pour l'ensemble de données Device Detail et définir l'intervalle entre deux collectes de ce type.

- **COLL_DBD_FRENAME_RETRY_CNT** : utilisez cette variable d'environnement pour indiquer le nombre de tentatives qui peuvent être effectuées pour déplacer le fichier %COLL_HOME%_tmp_%COLL_VERSION%_ %COLL_SERVERID%_%COLL_SERVERID%__DEVD_TEMP vers le fichier %COLL_HOME%_tmp_%COLL_VERSION%_ %COLL_SERVERID%_%COLL_SERVERID%__DEVD_PREV.

Si vous n'indiquez pas de valeur pour cette variable, l'agent Microsoft SQL Server fait une tentative de déplacement du fichier.

Variables d'optimisation de la collecte de l'ensemble de données MS SQL Database Detail

Pour optimiser la collecte de l'ensemble de données MS SQL Database Detail, utilisez les variables d'environnement suivantes :

- **COLL_KOQDBD_INTERVAL** : utilisez cette variable d'environnement pour indiquer un intervalle (en minutes) entre deux collectes basées sur une unité d'exécution consécutives de l'ensemble de données MS SQL Database Detail. Si vous n'indiquez pas de valeur pour cette variable ou si l'intervalle de temps spécifié est inférieur à 3 minutes, l'agent Microsoft SQL Server définit l'intervalle par défaut sur 3 minutes. Au cas où la collecte prend plus de temps, ou que les données sont fréquemment vues comme NOT_COLLECTED, vous pouvez vérifier la durée de la collecte en vous référant au journal `Database Detail Collection completed in %d seconds` et définir la valeur de la variable sur une valeur supérieure à la durée de collecte spécifiée dans le journal.
- **COLL_DBD_FRENAME_RETRY_CNT** : utilisez cette variable d'environnement pour indiquer le nombre de tentatives qui peuvent être effectuées pour déplacer le fichier %COLL_HOME%_tmp_%COLL_VERSION%_ %COLL_SERVERID%_%COLL_SERVERID%__DBD_TEMP vers le fichier %COLL_HOME%_tmp_%COLL_VERSION%_ %COLL_SERVERID%_%COLL_SERVERID%__DBD_PREV.

Si vous n'indiquez pas de valeur pour cette variable, l'agent Microsoft SQL Server fait une tentative de déplacement du fichier.

Variables d'optimisation de la collecte de l'ensemble de données MS SQL Database Details

Pour améliorer la collecte de l'ensemble de données MS SQL Database Details, utilisez les variables d'environnement suivantes :

- **COLL_AUDIT_TYPE** : utilisez cette variable pour activer ou désactiver la surveillance de journaux spécifiques. La valeur par défaut de la variable est [AL][FL][SL]. Par défaut, l'agent surveille les trois types de journaux qui comprennent les journaux d'application, les fichiers de contrôle et les journaux de sécurité. La valeur de la variable inclut un code de deux caractères pour chaque type de journal :
  - [AL] pour les journaux d'application
  - [FL] pour les fichiers de contrôle
  - [SL] pour les journaux de sécurité

  Vous pouvez modifier la valeur de la variable afin de désactiver la surveillance du type de journal spécifique. Par exemple, si vous indiquez [AL][SL] comme valeur de la variable, les fichiers de contrôle ne sont pas surveillés. Si aucune valeur n'est associée à la variable, les détails de l'audit ne sont pas surveillés.
- **COLL_AUDIT_DURATION** : utilisez cette variable pour signaler les événements d'audit qui se sont produits lors de l'intervalle indiqué dans cette variable. Par exemple, si vous attribuez la valeur 7 à cette variable, les événements d'audit qui se sont produits au cours des sept dernières heures sont signalés par l'ensemble de données Détails de l'audit. La valeur par défaut de la variable **COLL_AUDIT_DURATION** est `24 heures`.
- **COLL_AUDIT_COLLECTION_INTERVAL** : la collecte basée sur les unités d'exécution de l'ensemble de données Détails de l'audit fournit les spécifications de toutes les bases de données incluses dans l'instance SQL Server. Utilisez cette variable pour définir l'intervalle de cette collecte basée sur des unités d'exécution.

Par exemple, si vous attribuez la valeur 7 à cette variable, un nouvel ensemble de spécifications de base de données est extrait de l'instance SQL Server toutes les 7 heures. La valeur par défaut de la variable **COLL_AUDIT_COLLECTION_INTERVAL** est 24.

Variable d'optimisation de la collecte pour l'ensemble de données MS SQL Process Detail

Pour améliorer la collecte de l'ensemble de données MS SQL Process Detail, utilisez la variable **COLL_PROC_BLOCK_INTERVAL** avec les valeurs suivantes :

- Si **COLL_PROC_BLOCK_INTERVAL = 0**, la collecte pour les attributs Durée du processus de blocage et Durée de ressource de blocage est désactivée.
- Si **COLL_PROC_BLOCK_INTERVAL =** *x*, l'intervalle entre les deux collectes de données consécutives pour les attributs Durée du processus de blocage et Durée de ressource de blocage est *x* minutes.

Si la variable **COLL_PROC_BLOCK_INTERVAL** n'est pas définie dans le répertoire CANDLE_HOME, l'intervalle entre les collectes de données consécutives est trois minutes.

Variable permettant l'exclusion d'objets verrouillés de la collecte de données

Si les requêtes envoyées pour les espaces de travail Détails de base de données, Détails des groupes de fichiers, Fonction miroir de la base de données et Détails des unités mettent du temps à s'exécuter, utilisez la variable **COLL_DBCC_NO_LOCK** pour exécuter une requête avec la valeur WITH (NOLOCK). Cette variable permet à la requête de ne pas attendre dans la file d'attente lorsqu'un objet sur lequel elle s'exécute est verrouillé.

Variable permettant de définir les critères de recherche des lignes renvoyées par l'ensemble de données Détails de la table

Les lignes renvoyées par l'ensemble de données Détails de la table sont triées par ordre décroissant en fonction de la valeur définie pour la variable **COLL_TBLD_SORTBY**. La valeur par défaut de la variable **COLL_TBLD_SORTBY** est FRAG (pourcentage de fragmentation). Les valeurs admises sont ROWS (nombre de lignes dans une table), SPACE (espace utilisé par la table) et OPTSAGE (date des statistiques de l'optimiseur de la table).

Variable d'optimisation de la collecte pour les ensembles de données MS SQL Problem Detail et Problem Summary

- **COLL_ALERT_SEV** : utilisez cette variable pour définir le niveau de gravité des messages d'erreur affichés dans les ensembles de données Problem Detail et Problem Summary. Les messages d'erreur dont le niveau de gravité est supérieur ou égal à la valeur indiquée dans cette variable sont affichés dans les ensembles de données Problem Detail et Problem Summary. Par exemple, si vous définissez la valeur 10 pour cette variable, les messages d'erreur dont le niveau de gravité est supérieur ou égal à 10 sont affichés dans les ensembles de données Problem Detail et Problem Summary. Si vous n'indiquez pas de valeur pour cette variable, les messages d'erreur dont le niveau de gravité est supérieur ou égal à 17 sont affichés dans les ensembles de données Problem Detail et Problem Summary.
- **COLL_SINCE_ERRORLOG_RECY** : utilisez cette variable pour surveiller uniquement les erreurs dont le niveau de gravité est élevé dans le fichier ERRORLOG. Si vous n'indiquez pas de valeur pour cette variable, la valeur de la variable est 0, ce qui signifie que pour la collecte des données, l'ensemble de données Problem Summary prend en compte les erreurs de gravité élevée qui sont lues dans le fichier ERRORLOG précédent. Pour surveiller uniquement les erreurs dont le niveau de gravité est élevé dans le fichier ERRORLOG en cours, définissez cette variable en indiquant la valeur 1.

Variables de définition de l'intervalle du délai d'attente

Pour définir l'intervalle du délai d'attente pour l'agent Microsoft SQL Server, vous pouvez utiliser les variables d'environnement suivantes :

- **WAIT_TIMEOUT** : utilisez cette variable pour définir le délai d'attente de l'agent Microsoft SQL Server. Si un ensemble de données prend plus de 45 secondes pour collecter des données, l'agent risque de se bloquer ou le déclenchement de situations risque d'être incorrect. Examinez le journal afin d'identifier les ensembles de données qui prennent plus de 45 secondes pour collecter les données et utilisez la variable **WAIT_TIMEOUT** pour augmenter le délai d'attente entre la procédure de l'agent et la procédure du collecteur.
- **COLL_DB_TIMEOUT** : utilisez cette variable pour définir le délai d'attente (en secondes) de n'importe quelle demande, comme l'exécution d'une requête sur une connexion de serveur SQL existante à effectuer avant de revenir à l'application. Si vous indiquez la valeur `0`, il n'y a pas de délai d'attente. Si vous n'indiquez pas de valeur pour cette variable, l'agent attend 15 secondes avant de revenir à l'application.

Variables permettant de définir les propriétés des fichiers journaux du collecteur

Pour définir les propriétés des fichiers journaux du collecteur, vous pouvez utiliser les variables d'environnement suivantes :

- **COLL_WRAPLINES** : cette variable permet d'indiquer le nombre maximal de lignes dans le fichier `col.out`. La valeur par défaut de cette variable est 90000 lignes (2 Mo environ).
- **COLL_NUMOUTBAK** : cette variable permet d'indiquer le nombre de copies de sauvegarde des fichiers journaux du collecteur à créer. Par défaut, cinq copies de sauvegarde du fichier journal du collecteur sont créées. Le fichier de sauvegarde s'appelle `*.out`. Lorsque ce fichier de sauvegarde atteint sa taille maximale, il est renommé `*.ou1` et les derniers journaux sont placés dans le fichier `*.out`. Ainsi, pour cinq fichiers de sauvegarde, les journaux les plus anciens sont disponibles dans le fichier `*.ou5` et les journaux les plus récents sont disponibles dans le fichier `*.out`.

  Vous pouvez créer plus de cinq copies de sauvegarde des fichiers journaux du collecteur en indiquant l'une des valeurs suivantes dans la variable **COLL_NUMOUTBAK** :
  - Pour moins de dix fichiers de sauvegarde, indiquez le nombre de fichiers de sauvegarde que vous souhaitez créer dans la variable **COLL_NUMOUTBAK**. Par exemple, si vous indiquez `9` dans la variable **COLL_NUMOUTBAK**, neuf fichiers de sauvegarde sont créés.
  - Si le nombre de fichiers de sauvegarde est supérieur à 9 et inférieur à 1000, indiquez le nombre de fichiers de sauvegarde précédé par un tiret dans la variable **COLL_NUMOUTBAK**. Par exemple, si vous indiquez `-352` dans la variable **COLL_NUMOUTBAK**, 352 fichiers de sauvegarde sont créés.
- **COLL_DEBUG** : utilisez cette variable pour activer le suivi complet du collecteur en attribuant cette variable à la valeur `ddddddddddd` (10 fois «d»).

Variable de suppression des fichiers temporaires

COLL_TMPFILE_DEL_INTERVAL : cette variable permet d'indiquer l'intervalle (en minutes) au-delà duquel les fichiers temporaires `KOQ_<horodatage>` doivent être supprimés. Si vous n'indiquez pas de valeur pour cette variable, la valeur de la variable est `0`, ce qui signifie que les fichiers temporaires doivent être supprimés immédiatement.

Variable pour le changement de pilote utilisée par l'agent MS SQL Server

Pour changer le pilote utilisé par l'agent Microsoft SQL Server, utilisez la variable d'environnement **KOQ_ODBC_DRIVER**. Cette variable spécifie le pilote utilisé par l'agent Microsoft SQL Server pour se connecter au serveur SQL. Si vous n'indiquez pas de valeur pour cette variable, l'agent utilise le pilote ODBC SQL Server comme pilote par défaut.

Remarque : Lorsque vous spécifiez le pilote Microsoft SQL Server, vérifiez que le nom du pilote est correct et que le pilote est répertorié sous l'option correspondante dans la source de données (ODBC).

Configuration de l'agent en utilisant le fichier de réponses silencieux

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent. Vous pouvez également configurer plusieurs instances de l'agent à l'aide du fichier de réponses silencieux.

Avant de commencer

Pour configurer plusieurs instances de l'agent, vérifiez que les détails de configuration de toutes les instances de l'agent sont spécifiés dans le fichier de réponses silencieux.

Pourquoi et quand exécuter cette tâche

Exécutez le script de configuration pour modifier les paramètres de configuration. Vous pouvez modifier le fichier de réponses silencieux avant d'exécuter le script de configuration.

Procédure

Pour configurer l'agent, procédez comme suit :

1. Ouvrez le fichier `mssql_silent_config.txt` situé dans *rép_install*`\samples` et spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.
2. Ouvrez l'invite de commande et entrez la commande suivante :

   rép_install`\BIN\mssql-agent.bat config install_dir\samples\mssql_silent_config.txt`
3. Démarrez l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Exécution de l'agent dans un environnement cluster

Vous pouvez configurer l'agent Microsoft SQL Server dans un environnement cluster. Plusieurs instances de Microsoft SQL Server et d'agent Microsoft SQL Server peuvent s'exécuter sur un noeud unique.

Après avoir installé et configuré l'agent Microsoft SQL Server, procédez comme suit pour exécuter l'agent dans un environnement cluster :

- Ajoutez des variables d'environnement
- Modifiez le type de démarrage du service d'agent et du service de collecteur
- Ajoutez l'agent et le collecteur à l'environnement cluster

Vous pouvez configurer un environnement en cluster pour les versions suivantes de Microsoft SQL Server :

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016

Important : Sur les systèmes Windows, l'agent doit être installé dans le même répertoire que l'agent de système d'exploitation. Installez l'agent sur le disque système de noeuds de chaque noeud de cluster.

Ajout de variables d'environnement

Vous devez configurer les variables d'environnement qui sont utilisées par les agents qui sont installés sur chaque noeud de cluster.

Pourquoi et quand exécuter cette tâche

Vous devez définir les variables d'environnement suivantes :

- *CTIRA_HOSTNAME* : Cette variable est utilisée pour configurer chaque instance de l'agent Microsoft SQL Server. La valeur de cette variable est limitée à 31 caractères et est commune à tous les agents de surveillance. Définissez la valeur de cette variable sur le nom de cluster pour accéder à tous les agents de surveillance de ce cluster dans Tableau de bord d'Application Performance.
- *CTIRA_NODETYPE* : Cette variable est utilisée pour identifier l'agent. Par défaut, la valeur de cette variable est définie sur **MSS** pour l'agent Microsoft SQL Server.
- *CTIRA_SUBSYSTEMID* : La variable est utilisée pour distinguer plusieurs instances de l'agent Microsoft SQL Server. Par défaut, la valeur de cette variable est définie sur **Microsoft SQL Virtual Server** pour l'agent Microsoft SQL Server.
- *COLL_HOME* : Cette variable est utilisée pour collecter des données et pour stocker des fichiers journaux pour les groupes d'attributs qui utilisent des fichiers de configuration à un emplacement partagé. Définissez la valeur de la variable sur *X*`:\shared-location`, où *X* est une unité partagée accessible aux noeuds de cluster. Par exemple, définissez la valeur pour la variable *COLL_HOME* quand vous définissez les paramètres de configuration pour le groupe d'attributs Détails des tables MS SQL ou le groupe d'attributs Détails des événements d'erreur MS SQL.
- *CTIRA_HIST_DIR* : Cette variable est utilisée pour spécifier le chemin vers le répertoire de disque partagé. Si l'historique de l'agent Microsoft SQL Server est configuré pour être stocké sur l'agent de surveillance, chaque instance de l'agent doit être configurée avec une variable *CTIRA_HIST_DIR* commune qui fait référence au répertoire de disque partagé.

  A faire : Si l'historique est stocké sur le serveur Cloud APM, vous n'avez pas besoin d'indiquer une valeur pour la variable *CTIRA_HIST_DIR*. Le fait de stocker l'historique sur le serveur Cloud APM augmente la charge sur ce serveur.

Pour ajouter ces variables, consultez les étapes décrites dans «Définition des variables d'environnement local», à la page 521.

Que faire ensuite

Changez le type de démarrage du service d'agent et du service de collecteur sur **Manuel** en suivant les étapes décrites dans «Modification du type de démarrage du service d'agent et du service de collecteur».

Modification du type de démarrage du service d'agent et du service de collecteur

Par défaut, le type de démarrage du service d'agent et du service de collecteur est **Automatique**. Changez le type de démarrage du service d'agent et du service de collecteur sur **Manuel** de sorte que la ressource de cluster puisse contrôler le démarrage et l'arrêt de l'agent de surveillance

Procédure

Pour modifier le type de démarrage du service d'agent, effectuez les étapes suivantes :

1. Cliquez sur **Démarrer** > **Exécuter**, puis entrez la commande `services.msc` et cliquez sur **OK**.
2. Cliquez avec le bouton droit de la souris sur l'agent, puis cliquez sur **Propriétés**.
3. Dans la liste **Type de démarrage** de la fenêtre de propriétés de l'agent de surveillance pour Microsoft SQL Server, sélectionnez **Manuel**, cliquez sur **Appliquer** puis sur **OK**.

Que faire ensuite

- Employez la même procédure pour changer le type de démarrage du service de collecteur en **Manuel**.
- Ajoutez l'agent et le collecteur à l'environnement cluster en suivant les étapes décrites dans «Ajout de l'agent et du collecteur à l'environnement cluster».

Ajout de l'agent et du collecteur à l'environnement cluster

Vous devez ajouter l'agent et le collecteur à l'environnement cluster.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Gestion du cluster de basculement**.
2. Développez **Gestion du cluster de basculement**.
3. Développez **Services et applications** et cliquez avec le bouton droit de la souris sur l'instance SQL à configurer.
4. Cliquez sur **Ajouter une ressource > Service générique**. L'assistant Nouvelle ressource s'affiche.
5. Sur la page de sélection du service, sélectionnez le nom du service, puis cliquez sur **Suivant**.

   Exemple de noms de services Windows :

   - `Agent de surveillance pour Microsoft SQL Server : SQLTEST#INSTANCE1`
   - `Agent de surveillance pour Microsoft SQL Server : Collector SQLTEST#INSTANCE1`
   - `Agent de surveillance pour Microsoft SQL Server : SQLTEST2#INSTANCE2`
   - `Agent de surveillance pour Microsoft SQL Server : Collector SQLTEST2#INSTANCE2`
6. Sur la page de confirmation, contrôlez les détails, puis cliquez sur **Suivant**.
7. Dans la page Récapitulatif, cliquez sur **Terminer**. Le agent Microsoft SQL Server est maintenant ajouté.

   A faire : Utilisez les mêmes étapes pour ajouter le collecteur à l'environnement cluster.
8. Pour remettre l'agent en ligne, cliquez avec le bouton droit de la souris sur l'agent, puis cliquez sur l'option permettant de **mettre cette ressource en ligne**.
9. Pour remettre le collecteur en ligne, cliquez avec le bouton droit de la souris sur le collecteur, puis cliquez sur l'option permettant de **mettre cette ressource en ligne**.

Résultats

L'agent Microsoft SQL Server est dorénavant en cours d'exécution dans un environnement cluster.

A faire : Si vous voulez configurer l'agent de nouveau, vous devez d'abord mettre l'agent et le collecteur hors ligne, ou éditer les variables d'agent sur le noeud sur lequel ils s'exécutent. Une fois que vous avez terminé la configuration de l'agent, remettez l'agent et le collecteur en ligne.

Configuration de l'agent à l'aide de l'utilitaire Cluster

L'utilitaire cluster vous permet d'ajouter plusieurs instances d'agent Microsoft SQL Server à un groupe de clusters dans un environnement cluster.

L'utilitaire Cluster ajoute automatiquement le service d'agent et le service de collecteur de chaque instance d'agent Microsoft SQL Server en tant que ressource de service générique au groupe de clusters. L'utilitaire cluster vous permet de réaliser les tâches suivantes :

- Ajout d'une instance d'agent SQL Server au cluster
- Mise à jour d'une instance existante d'agent SQL Server dans un cluster
- Suppression d'une instance d'agent SQL Server à partir d'un cluster

Prérequis pour l'utilisation de l'utilitaire Cluster

Vous devez vous assurer que votre environnement système satisfait aux prérequis pour l'exécution de l'utilitaire Cluster.

Assurez-vous que les prérequis suivants sont respectés :

- Exécutez l'utilitaire Cluster sur un ordinateur disposant d'au moins un groupe dans l'environnement cluster.
- Démarrez le service de registre distant pour tous les noeuds dans la grappe.
- Vous devez avoir l'autorisation de gestionnaire de grappes pour accéder à l'utilitaire Cluster.
- Le nom de service de l'agent et du collecteur doit être identique sur tous les noeuds de cluster.

  Par exemple, si le nom de service de l'agent est Monitoring Agent for Microsoft SQL Server : `SQLTEST#INSTANCE1` et que le nom du collecteur est Monitoring Agent for Microsoft SQL Server : Collecteur `SQLTEST#INSTANCE1`, le même nom de service doit figurer sur tous les noeuds du cluster.

Ajout d'une instance d'agent Microsoft SQL Server au cluster

L'utilitaire cluster vous permet d'ajouter une instance d'agent Microsoft SQL Server à un groupe de clusters dans un environnement cluster.

Procédure

1. Pour exécuter l'utilitaire, exécutez l'une des étapes suivantes :
   - Dans le cas d'un agent 64 bits, accédez au répertoire *rép_base_candle*`\TMAITM6_x64`.
   - Dans le cas d'un agent 32 bits, accédez au répertoire *rép_base_candle*`\TMAITM6`.
2. Cliquez deux fois sur `KoqClusterUtility.exe` pour lancer l'utilitaire Cluster.
3. Dans la zone SQL **Server Agent Instances Available**, sélectionnez une instance d'agent Microsoft SQL Server, puis cliquez sur **Add**.
4. Dans la fenêtre Select cluster group name, sélectionnez un groupe de clusters. Le groupe de clusters que vous sélectionnez doit être l'instance de SQL Server surveillée par l'agent Microsoft SQL Server.
5. Dans la fenêtre Select Path for Shared Location, naviguez jusqu'à l'emplacement de stockage des journaux de l'agent et du collecteur. Si vous n'avez pas sélectionné de chemin d'accès, l'emplacement `CANDLEHOME/TMAITM6(_x64)/logs` est sélectionné par défaut pour stocker les journaux d'agent et de collecteur.
6. Pour ajouter l'instance d'agent Microsoft SQL Server à l'environnement cluster, cliquez sur **OK**. Les journaux d'activité de l'utilitaire Cluster s'affichent dans le panneau Historique.

Mise à jour d'une instance d'agent Microsoft SQL Server existante dans un cluster

L'utilitaire cluster vous permet de mettre à jour l'emplacement de stockage des journaux de l'agent et du collecteur pour une instance de SQL Server dans un cluster.

Procédure

1. Pour mettre à jour une instance d'agent Microsoft SQL Server existante, accédez à la fenêtre Cluster Utility.
2. Dans la zone **SQL Server Agent Instances Configured**, sélectionnez une instance d'agent Microsoft SQL Server, puis cliquez sur **Update**.
3. Dans la fenêtre Set Path for Shared Location, naviguez jusqu'à l'emplacement de stockage des journaux de l'agent et du collecteur. Si vous ne sélectionnez pas le chemin d'accès, les journaux de l'agent et du collecteur sont stockés à l'emplacement qui a été défini lors de l'ajout de l'instance d'agent Microsoft SQL Server dans un cluster.
4. Cliquez sur **OK**. Les journaux d'activité de l'utilitaire Cluster s'affichent dans le panneau Historique.

Suppression d'une instance d'agent Microsoft SQL Server à partir d'un cluster

L'utilitaire cluster vous permet de supprimer une instance d'agent Microsoft SQL Server d'un groupe de clusters.

Procédure

1. Accédez à la fenêtre Cluster Utility.
2. Dans la zone **SQL Server Agent Instances Configured**, sélectionnez une instance d'agent Microsoft SQL Server, puis cliquez sur **Remove**.
3. Dans la boîte de dialogue **Please Confirm Action**, cliquez sur **Yes** pour supprimer l'instance d'agent Microsoft SQL Server du cluster. Les journaux d'activité de l'utilitaire Cluster s'affichent dans le panneau Historique.

Configuration de plusieurs classements pour le fichier ERRORLOG

L'agent Microsoft SQL Server version 06.31.17.00 (ou version ultérieure) pour Application Performance Management version 8.1.4.0.4 prend en charge les classements multiples dans le fichier `ERRORLOG`. Vous pouvez désormais configurer l'agent pour qu'il analyse plusieurs classements dans le fichier `ERRORLOG` pour le groupe d'attributs **Problem Detail**. Notez que les classements multiples dans le fichier `ERRORLOG` ne sont pas applicables pour le groupe d'attributs **Détails des événements d'erreur**.

Avant de commencer

Pour configurer plusieurs classements de l'agent, vérifiez que l'agent est installé.

Pourquoi et quand exécuter cette tâche

Le classement par défaut est Anglais. Pour les autres langues de SQL Server, l'agent analyse le fichier ERRORLOG en fonction des classements du fichier de configuration `koqErrConfig.ini`. Vous devez donc ajouter les classements utilisés dans le fichier `koqErrConfig.ini`.

Procédure

Pour configurer plusieurs classements pour l'agent, procédez comme suit :

1. Accédez au répertoire *répertoire_agent* de l'agent.
   - Pour l'agent 64 bits, *répertoire_agent* correspond à *rép_base_agent*`\TMAITM6_x64`.
   - Pour l'agent 32 bits, *répertoire_agent* correspond à *rép_base_agent*`\TMAITM6`.

   , *rép_base_agent* représentant le répertoire d'installation de l'agent.
2. Ouvrez le fichier `koqErrConfig.ini` de la configuration :
3. Accédez à la fin du fichier pour ajouter les nouveaux classements. Par exemple, pour activer le classement pour Français, ajoutez les paramètres de classement ci-après dans le format des paires **`name-value`** à la fin du fichier `koqErrConfig.ini`.

   ```
   [French]
   Error = Erreur :
   Severity = Gravité :
   State = Etat :
   ```

   Remarque : L'exemple de liste de classements est disponible dans *répertoire_agent*`\koqErrConfigSample.ini`.
   Où
   - Pour l'agent 64 bits, *répertoire_agent* correspond à *rép_base_agent*`\TMAITM6_x64`.
   - Pour l'agent 32 bits, *répertoire_agent* correspond à *rép_base_agent*`\TMAITM6`.

   , *rép_base_agent* représentant le répertoire d'installation de l'agent.

   Si le classement cible n'est pas disponible dans le fichier `koqErrConfigSample.ini`, vous pouvez déterminer les valeurs des mots clés de classement dans le fichier `ERRORLOG`.
   Respectez bien le format de classement ci-dessous pour configurer les paramètres de classement dans le fichier `koqErrConfig.ini`.

```
[nom_section]
Error = valeur_erreur
Severity = valeur_gravité
State = valeur_état
```

Où

- *nom_section* représente le nom du classement SQL Server. Vérifiez que le nom de classement est placé entre crochets **[]**.
- *valeur_erreur* représente le mot clé de l'erreur correspondante qui se trouve dans le fichier ERRORLOG de votre classement cible.
- *valeur_gravité* représente le mot clé de la gravité correspondante qui se trouve dans le fichier ERRORLOG de votre classement cible.
- *valeur_état* représente le mot clé de l'état correspondant qui se trouve dans le fichier ERRORLOG de votre classement cible.

Important : Les valeurs de mot clé sont sensibles à la casse et doivent être identiques à celles du fichier ERRORLOG, caractères spéciaux compris.

4. Sauvegardez le fichier koqErrConfig.ini de la configuration.

   Il n'est pas nécessaire de redémarrer l'agent.

   Si le fichier de configuration koqErrConfig.ini n'est pas disponible ou que le fichier de configuration koqErrConfig.ini est vide, le fichier ERRORLOG indique le classement par défaut sous forme de message d'erreur anglais dont le niveau de gravité est supérieur au niveau de gravité par défaut (s'il en existe un).

   Si le fichier de configuration koqErrConfig.ini est correctement configuré, le fichier ERRORLOG affiche les messages d'erreur correspondants dont le niveau de gravité est supérieur au niveau de gravité par défaut (s'il en existe un).

   Le niveau de gravité par défaut est de 17.

   Avertissement : Les modifications apportées au fichier koqErrConfig.ini ne sont pas conservées lors de la mise à niveau de l'agent ; vous devez effectuer une sauvegarde au préalable.

Que faire ensuite

Vérifiez le widget **Errorlog Alert** ou le groupe d'attributs **Problem Detail** sur le tableau de bord Application Performance Management qui résulte des paramètres de classement.

Configuration de la surveillance de MongoDB

L'Monitoring Agent for MongoDB a besoin d'un nom d'instance. Vous devez configurer et démarrer manuellement l'instance d'agent. L'Agent MongoDB prend en charge la surveillance locale et la surveillance à distance. Prenez connaissance des prérequis suivants pour configurer l'Agent MongoDB en vue de la surveillance locale et de la surveillance à distance.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent MongoDB.
- Assurez-vous que l'utilisateur qui configure l'Agent MongoDB dispose des rôles permettant de collecter les données pour l'ensemble des attributs.
  - Pour configurer l'agent sur la version 2.4 et la version 2.6 de la base de données MongoDB, les rôles clusterAdmin, readAnyDatabase et dbAdminAnyDatabase doivent être affectés à l'utilisateur
  - Pour configurer l'agent sur la version 3.x de la base de données MongoDB, les rôles clusterMonitor, readAnyDatabase et dbAdminAnyDatabase doivent être affectés à l'utilisateur

Pour en savoir plus sur les groupes d'attributs pour lesquels ces rôles utilisateur sont requis, voir tableau 142.

- Utilisez un utilisateur existant ou créez-en un dans la base de données d'administration. Avant de créer un utilisateur et de lui attribuer des rôles, vous devez vous connecter à la base de données MongoDB et changer la base de données en base de données d'administration.

  Important : Si le processus mongod ou mongos s'exécute en mode d'authentification, entrez les données d'identification requises pour vous connecter à la base de données MongoDB.

  1. Exécutez la commande suivante pour vous connecter à la base de données MongoDB :

     `mongo IP:port`

     Où
     - *IP* est l'adresse IP du processus mongod ou mongos
     - *port* est le numéro de port du processus mongod ou mongos
  2. Changez la base de données en base de données d'administration :

     `use admin`
  3. Exécutez l'une des commandes suivantes pour ajouter un utilisateur dans la base de données d'administration MongoDB, puis affectez les rôles requis à l'utilisateur :
     - Pour la base de données MongoDB version 2.4, exécutez la commande suivante :

       `db.addUser({ user: "nomutilisateur", pwd: "motdepasse", roles: [ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })`
     - Pour la base de données MongoDB version 2.6, exécutez la commande suivante :

       `b.createUser({user: "nomutilisateur", pwd: ""motdepasse"", roles: [ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })`
     - Pour la base de données MongoDB version 3.x, exécutez la commande suivante :

       `db.createUser({user: "nomutilisateur", pwd: "motdepasse", roles: [ 'clusterMonitor', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })`
  4. Exécutez la commande suivante pour vérifier que l'utilisateur a été ajouté à la base de données d'administration :

     `db.auth(nomutilisateur, motdepasse)`

     Le code retour **`1`** indique que l'utilisateur est ajouté, tandis que le code retour **`0`** indique que l'ajout de l'utilisateur a échoué.

Le tableau suivant contient des informations sur les rôles utilisateur et sur les attributs pour lesquels ils sont requis :

Tableau 142. Groupes d'attributs et leurs rôles utilisateur requis

Rôles	Version de base de données MongoDB	Groupes d'attributs
dbAdminAnyDatabase	2.x et 3.x	Temps de réponse
readAnyDatabase	2.x et 3.x	• Liste Mongod • Informations générales sur les fragments • Stockage des collectes • Noms de base de données

Tableau 142. Groupes d'attributs et leurs rôles utilisateur requis (suite)

Rôles	Version de base de données MongoDB	Groupes d'attributs
clusterAdmin	2.x	• Informations d'instance Mongo • Infos d'E-S d'instance Mongo • MII Copy For APMUI One • MII Copy For APMUI Two • Verrou de BD d'instance Mongo • Verrous • Verrous MongoDB • Détails WiredTiger • Détails MMAPv1
clusterMonitor	3.x	• Informations d'instance Mongo • Infos d'E-S d'instance Mongo • MII Copy For APMUI One • MII Copy For APMUI Two • Verrou de BD d'instance Mongo • Verrous • Verrous MongoDB • Détails WiredTiger • Détails MMAPv1

- Pour la surveillance à distance du serveur MongoDB, prenez connaissance des deux prérequis suivants :
  1. L'agent MongoDB est installé et configuré sur le système où le serveur de base de données MongoDB est installé pour la surveillance à distance.
  2. Le fichier `/etc/hosts` du système hébergeant l'agent contient une entrée pour la machine distante.

Pourquoi et quand exécuter cette tâche

Le nom du système géré inclut le nom d'instance que vous indiquez. Par exemple, vous pouvez spécifier le nom d'instance sous la forme *nom_instance*`:`*nom_hôte*`:`*cp*, où *cp* est le code produit à deux caractères de votre agent. Le nom de système géré admet jusqu'à 32 caractères. Le nom d'instance admet jusqu'à 28 caractères, moins la longueur du nom d'hôte. Par exemple, si vous indiquez `Mongo2` comme nom d'instance, le nom du système géré est `Mongo2:hostname:KJ`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 143. Versions d'agent et documentation

Version de l'Agent MongoDB	Documentation
1.0.0.12	IBM Cloud Application Performance Management
1.0.0.10	IBM Performance Management 8.1.3 *
1.0.0.9	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

A faire :

- Pour que l'agent collecte correctement les données, démarrez-le en tant que superutilisateur (root) ou utilisez le même ID utilisateur pour démarrer l'agent et le processus mongod.
- Dans un environnement où MongoDB fonctionne comme cluster, veillez à installer l'agent sur le même ordinateur que celui où s'exécute le processus de routeur. Configurez l'agent sur le même ordinateur avec l'adresse IP et le numéro de port de ce dernier et définissez **TYPE** à la valeur 1.
- Dans un environnement où MongoDB fonctionne comme cluster en mode d'authentification, ajoutez bien le même ID utilisateur avec les droits requis sur tous les fragments du cluster.

Vous pouvez configurer l'agent en utilisant les paramètres par défaut, en éditant le fichier de réponses silencieux ou en répondant aux invites.

Configuration de l'agent avec les paramètres par défaut

Dans un environnement typique, utilisez les paramètres par défaut pour configurer l'agent. Lorsque les paramètres par défaut sont utilisés pour la configuration de l'agent, ce dernier ne s'exécute pas en mode d'authentification.

Procédure

1. Exécutez la commande suivante :
   rép_install/bin/mongodb-agent.sh config *nom_instance rép_install*/samples/mongodb_silent_config.txt

   Où

   - *nom_instance* est le nom que vous spécifiez pour l'instance d'application unique.
   - *rép_install* correspond au répertoire d'installation de l'Agent MongoDB.

   Le répertoire d'installation par défaut est /opt/ibm/apm/agent.
2. Exécutez la commande suivante pour démarrer l'agent :
   rép_install/bin/mongodb-agent.sh start *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour définir des valeurs différentes pour les paramètres de configuration, et configurer l'agent.

Avant de commencer

Pour exécuter la base de données MongoDB dans le mode d'authentification, veillez à configurer l'agent avec un identificateur disposant des rôles clusterAdmin, readAnyDatabase et dbAdminAnyDatabase sur la base de données MongoDB.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant :
   rép_install/samples/mongodb_silent_config.txt.

2. Pour le paramètre **TYPE**, entrez l'une des valeurs suivantes :
   - 1 pour un cluster
   - 2 pour un ensemble de réplication
   - 3 pour une instance autonome

   Par défaut, l'agent surveille un cluster.
3. Pour le paramètre **PORT**, indiquez le numéro de port du routeur d'un cluster MongoDB ou d'une instance mongod de l'ensemble de réplication MongoDB surveillé.

   A faire : Si vous n'indiquez pas de numéro de port, l'agent reconnaît automatiquement le numéro de port du processus MongoDB approprié qui est actif dans l'interface par défaut. S'il n'y a pas de processus MongoDB actif dans l'interface par défaut, l'agent sélectionne le numéro de port du processus MongoDB approprié qui est actif dans la seconde interface.
4. Pour le paramètre **HOST**, indiquez l'adresse IP du système hôte MongoDB.

   A faire : Si vous n'indiquez pas d'adresse IP, l'agent détecte automatiquement l'adresse IP du processus MongoDB approprié qui est actif dans l'interface par défaut. Si le processus MongoDB est actif dans l'interface par défaut, l'agent détecte l'adresse IP du processus MongoDB approprié qui est actif dans l'interface secondaire.
5. Pour le paramètre **AUTHENTICATION**, indiquez YES pour spécifier que MongoDB est exécuté dans le mode d'authentification. La valeur par défaut est NO, qui indique que l'agent ne s'exécute pas actuellement en mode d'authentification.

   A faire : Lorsque la base de données MongoDB s'exécute en mode d'authentification, l'Agent MongoDB ou un client MongoDB ne peut pas se connecter à celle-ci sans données d'identification. Pour vous connecter à la base de données qui s'exécute en mode d'authentification, spécifiez YES pour le paramètre **AUTHENTICATION**.

   Si vous indiquez YES, effectuez les opérations suivantes :
   a. Pour le paramètre **User Name**, indiquez le nom d'utilisateur du routeur ou l'instance mongod. Assurez-vous que les rôles minimaux sont affectés à l'utilisateur. Pour plus d'informations sur les rôles d'utilisateur, voir tableau 142, à la page 534.
   b. Pour le paramètre **Password**, indiquez le mot de passe.
6. Sauvegardez et fermez le fichier mongodb_silent_config.txt, puis exécutez la commande suivante : *rép_install*/bin/mongodb-agent.sh config *nom_instance rép_install*/samples/mongodb_silent_config.txt

   Où
   - *nom_instance* est le nom que vous donnez à l'instance.
   - *rép_install* correspond au répertoire d'installation de l'Agent MongoDB.
7. Exécutez la commande suivante pour démarrer l'agent : *rép_install*/bin/mongodb-agent.sh start *nom_instance*

   Important : Si vous mettez à niveau l'agent vers la version V1.0.0.9 ou ultérieure, et que vous voulez exécuter l'agent en mode d'authentification, vous devez reconfigurer l'agent afin d'indiquer un nom d'utilisateur et un mot de passe. Pour effectuer la collecte des données, vous devez arrêter et redémarrer l'agent après l'avoir configuré.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en répondant à des invites

Pour configurer l'agent avec des paramètres personnalisés, vous pouvez indiquer des valeurs pour les paramètres de configuration lorsque le système vous y invite pendant que le script est en cours d'exécution.

Procédure

1. Exécutez la commande suivante :
   rép_install/bin/mongodb-agent.sh config *nom_instance*

   Où

   - *nom_instance* est le nom que vous donnez à l'instance.
   - *rép_install* correspond au répertoire d'installation de l'Agent MongoDB.
2. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **TYPE**, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez l'une des valeurs suivantes et appuyez ensuite sur la touche Entrée:

   - 1 pour un cluster
   - 2 pour un ensemble de réplication
   - 3 pour une instance autonome

   Par défaut, l'agent surveille un cluster.
3. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **PORT**, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez le numéro de port du routeur pour un cluster MongoDB ou une instance mongod de l'ensemble de réplication MongoDB qui est surveillé, puis appuyez sur Entrée.

   A faire : Si vous n'indiquez pas de numéro de port, l'agent reconnaît automatiquement le numéro de port du processus MongoDB approprié qui est actif dans l'interface par défaut. S'il n'y a pas de processus MongoDB actif dans l'interface par défaut, l'agent sélectionne le numéro de port du processus MongoDB approprié qui est actif dans la seconde interface.
4. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **HOST**, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez l'adresse IP du système hôte MongoDB et appuyez ensuite sur la touche Entrée.

   A faire : Si vous n'indiquez pas d'adresse IP, l'agent détecte automatiquement l'adresse IP du processus MongoDB approprié qui est actif dans l'interface par défaut. Si le processus MongoDB est actif dans l'interface par défaut, l'agent détecte l'adresse IP du processus MongoDB approprié qui est actif dans l'interface secondaire.
5. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **AUTHENTICATION**, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez si l'agent s'exécute en mode d'authentification.

   La valeur par défaut est NO, qui indique que l'agent ne s'exécute pas actuellement en mode d'authentification. Spécifiez YES pour indiquer que mongoDB s'exécute en mode d'authentification.

   A faire : Lorsque la base de données MongoDB s'exécute en mode d'authentification, l'Agent MongoDB ou un client MongoDB ne peut pas se connecter à celle-ci sans données d'identification. Pour vous connecter à la base de données qui s'exécute en mode d'authentification, spécifiez YES pour le paramètre **AUTHENTICATION**.

   Si vous indiquez YES, effectuez les opérations suivantes :

   a. Pour le paramètre **User Name**, indiquez le nom d'utilisateur du routeur ou l'instance mongod. Assurez-vous que les rôles minimaux sont affectés à l'utilisateur. Pour plus d'informations sur les rôles d'utilisateur, voir tableau 142, à la page 534.

b. Pour le paramètre **Password**, indiquez le mot de passe.

6. Exécutez la commande suivante pour démarrer l'agent :
   rép_install/bin/mongodb-agent.sh start *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de la surveillance de MySQL

L'Monitoring Agent for MySQL requiert un nom d'instance et les données d'identification utilisateur pour le serveur MySQL. Vous pouvez modifier les paramètres de configuration après avoir créé la première instance d'agent.

Avant de commencer

- Assurez-vous qu'un utilisateur est créé dans la base de données MySQL pour exécuter l'agent. L'utilisateur n'a pas besoin de privilèges particuliers sur la base de données MySQL surveillée.
- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent MySQL.

Pourquoi et quand exécuter cette tâche

Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Le nom de système géré admet jusqu'à 32 caractères. Le nom d'instance que vous entrez admet jusqu'à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous indiquez `MySQL2` comme nom d'instance, le nom du système géré est `MySQL2:hostname:SE`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant ici concernent l'édition la plus récente de l'agent, sauf indication contraire. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 144. Versions d'agent et documentation

Version de l'Agent MySQL	Documentation
1.0.0.10	IBM Cloud Application Performance Management
1.0.0.9	IBM Performance Management 8.1.3 *

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer>Tous les programmes>IBM Monitoring agents>IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, procédez comme suit :
   a. Cliquez deux fois sur le modèle **Agent de surveillance pour MySQL**.
   b. Dans la fenêtre Agent de surveillance pour MySQL indiquez un nom d'instance et cliquez sur **OK**.
3. Dans la fenêtre Agent de surveillance pour MySQL, procédez comme suit :
   a. Dans la zone **Adresse IP**, entrez l'adresse IP d'un serveur MySQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.
   b. Dans la zone **Nom d'utilisateur JDBC**, entrez le nom d'un utilisateur du serveur MySQL. La valeur par défaut est root.
   c. Dans la zone **Mot de passe JDBC**, entrez le mot de passe d'un utilisateur JDBC.
   d. Dans la zone **Confirmer le mot de passe JDBC**, entrez de nouveau le mot de passe.
   e. Dans la zone **Fichier Jar JDBC**, cliquez sur **Parcourir** et localisez le répertoire qui contient le fichier Java de connecteur MySQL, et sélectionnez-le.
   f. Cliquez sur **Suivant**.
   g. Dans la zone **Numéro de port JDBC**, indiquez le numéro de port du serveur JDBC. Le numéro de port par défaut est 3306.
   h. Dans la liste **Niveau de trace Java**, sélectionnez un niveau de trace pour Java. La valeur par défaut est `Error`.
   i. Cliquez sur **OK**. L'instance est affichée dans la fenêtre IBM Performance Management.
4. Cliquez avec le bouton droit de la souris sur l'instance **Agent de surveillance pour MySQL** et cliquez sur **Démarrer**.

   A faire : Pour configurer de nouveau l'agent, effectuez ces étapes dans la fenêtre IBM Performance Management :
   a. Arrêtez l'instance d'agent que vous voulez configurer.
   b. Cliquez avec le bouton droit de la souris sur l'instance **Agent de surveillance pour MySQL** et cliquez sur **Reconfigurer**.
   c. Répétez les étapes 3 et 4.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Linux

Exécutez le script de configuration pour configurer l'agent sur les systèmes Linux.

Procédure

1. Exécutez la commande suivante :

   ```
   rép_install/bin/mysql-agent.sh config nom_instance
   ```

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent MySQL.
2. A l'invite d'entrée d'une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez une autre valeur et appuyez sur Entrée.
   - Adresse IP
   - Nom d'utilisateur JDBC

- Mot de passe JDBC
- Ressaisir le mot de passe JDBC
- Fichier Jar JDBC
- Numéro du port JDBC (le numéro du port par défaut est 3306.)
- Niveau de trace Java (la valeur par défaut est `Error`.)

Pour plus d'informations sur les paramètres de configuration, voir «Configuration de l'agent en utilisant le fichier de réponses silencieux».

3. Exécutez la commande suivante pour démarrer l'agent.
   rép_install`/bin/mysql-agent.sh start` *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Utilisez le fichier de réponses silencieux pour configurer l'agent sans répondre aux invites quand vous exécutez le script de configuration. Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent sur les systèmes Windows et Linux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration. Vous éditez les valeurs de paramètre dans le fichier de réponses, et exécutez le script de configuration pour créer une instance d'agent et mettre à jour les valeurs de configuration.

Procédure

Windows Pour cette procédure, le chemin d'accès par défaut est celui où l'agent est installé :
Windows `C:\IBM\APM`
Linux `opt/ibm/apm/agent`
Si vous avez installé l'agent dans un autre chemin, remplacez le chemin dans les instructions et éditez le paramètre **`AGENT_HOME`** dans le fichier de réponses silencieux en spécifiant le chemin d'installation de l'agent.

1. Dans un éditeur de texte, ouvrez le fichier de réponses disponible à l'emplacement suivant :
   Linux *rép_install*`/samples/mysql_silent_config.txt`
   Windows *rép_install*`\samples\mysql_silent_config.txt`
   Où *rép_install* correspond au répertoire d'installation de l'Agent MySQL.
2. Dans le fichier de réponses, indiquez une valeur pour les paramètres suivants :
   - Pour le paramètre **`Nom de serveur`**, spécifiez l'adresse IP d'un serveur MySQL à surveiller à distance. Sinon, conservez la valeur par défaut `localhost`.
   - Pour le paramètre **`Nom d'utilisateur JDBC`**, conservez la valeur de nom d'utilisateur par défaut `root` ou indiquez le nom d'un utilisateur qui dispose des droits permettant d'afficher les tables INFORMATION_SCHEMA.
   - Pour le paramètre **`Mot de passe JDBC`**, entrez le mot de passe de l'utilisateur JDBC.
   - Pour le paramètre **`Fichier JAR JDBC`**, conservez le chemin par défaut si ce chemin d'accès au connecteur MySQL pour le fichier JAR Java est correct. Sinon, indiquez le chemin approprié. Le connecteur est disponible à l'emplacement par défaut suivant :
     Linux `/usr/share/java/mysql-connector-java.jar`

Windows C:\Program Files (x86)\MySQL\Connector J 5.1.26\mysql-connector-java-5.1.26-bin.jar

- Pour le paramètre **Numéro de port JDBC**, conservez le numéro de port par défaut 3306 ou indiquez un autre numéro de port.
- Pour le paramètre **Niveau de trace Java**, conservez la valeur par défaut Erreur ou indiquez un autre niveau de trace selon les instructions du support IBM.

3. Sauvegardez et fermez le fichier de réponses, puis entrez la commande suivante pour mettre à jour les paramètres de configuration de l'agent :

   Linux *rép_install*/bin/mysql-agent.sh config *nom_instance rép_install*/samples/mysql_silent_config.txt

   Windows *rép_install*\BIN\mysql-agent.bat config *nom_instance rép_install*\samples\mysql_silent_config.txt

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent MySQL.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, aucune donnée d'agent ne s'affiche dans les tableaux de bord.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de la surveillance de NetApp Storage

L'Monitoring Agent for NetApp Storage surveille les systèmes de stockage NetApp à l'aide de NetApp OnCommand Unified Manager, d'OnCommand API Services et d'OnCommand Performance Manager.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent NetApp Storage.
- Assurez-vous que les composants suivants sont installés sur votre machine :
  - OnCommand Unified Manager
  - OnCommand Performance Manager
  - OnCommand API Services

  Pour plus d'informations sur l'installation de ces composants, voir la documentation NetApp.
- Assurez-vous que les versions d'OnCommand API Services, d'OnCommand Unified Manager et d'OnCommand Performance Manager sont compatibles. Par exemple, pour configurer OnCommand API Services V1.0, associez OnCommand Unified Manager V6.2, V6.1 ou V6.0 à OnCommand Performance Manager V1.1. Pour connaître les versions de produit compatibles, voir Interoperability Matrix Tool.
- Assurez-vous que l'utilisateur qui se connecte à OnCommand Unified Manager dispose du privilège GlobalRead pour le système de stockage NetApp en cours de surveillance. Utilisez un ID utilisateur existant disposant de ce privilège ou créez un nouvel ID utilisateur. Pour plus d'informations sur la création de l'ID utilisateur dans votre système de stockage NetApp, voir la documentation NetApp.
- Assurez-vous que l'utilisateur que vous utilisez pour la configuration d'OnCommand API Services est un administrateur ou un contrôleur. Ces types d'utilisateur disposent par défaut des droits d'exécution de l'API REST.

- Téléchargez le fichier JAR de NetApp Manageability SDK (`manageontap.jar`) à partir du site Web de NetApp et installez le fichier dans le répertoire `lib` de l'agent de surveillance en procédant comme décrit à la rubrique «Téléchargement et installation du fichier JAR de NetApp Manageability SDK».

Pourquoi et quand exécuter cette tâche

L'agent NetApp Storage est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir agent NetApp Storage. Pour accéder à la documentation de la version 7.2.0.4, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Téléchargement et installation du fichier JAR de NetApp Manageability SDK

L'agent NetApp Storage nécessite que le fichier JAR de NetApp Manageability SDK communique avec un serveur NetApp OCUM.

Pourquoi et quand exécuter cette tâche

Après avoir installé l'agent NetApp Storage, téléchargez le fichier JAR de NetApp Manageability SDK (`manageontap.jar`) à partir du site Web de NetApp et installez le fichier dans le répertoire `lib` de l'agent de surveillance.

Procédure

1. Téléchargez le fichier compressé contenant le fichier JAR à partir du site Web suivant : http://communities.netapp.com/docs/DOC-1152.
2. Extrayez ce fichier compressé et copiez le fichier `manageontap.jar` aux emplacements suivants :
   - Pour les systèmes Windows 32 bits, copiez le fichier dans *rép_install*`/tmaitm6`
   - Pour les systèmes Windows 64 bits, copiez le fichier dans *rép_install*`/tmaitm6_x64`
   - Pour les systèmes Linux 32 bits, copiez le fichier dans *rép_install*`/li6263/nu/lib`
   - Pour les systèmes Linux x86-64 64 bits, copiez le fichier dans *rép_install*`/lx8266/nu/lib`
   - Pour les systèmes zLinux 64 bits, copiez le fichier dans *rép_install*`/ls3266/nu/lib`

Que faire ensuite

Terminez la configuration de l'agent.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'agent NetApp Storage fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for NetApp Storage**, puis sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Monitoring Agent for NetApp Storage, procédez comme suit :
   a. Entrez un nom unique pour l'instance de l'agent NetApp Storage et cliquez sur **OK**.
   b. Dans l'onglet **Fournisseur de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   c. Dans l'onglet **OnCommand Unified Manager**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   d. Dans l'onglet **OnCommand API Service**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Monitoring Agent for NetApp Storage, consultez les rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données», à la page 546
   - «Paramètres de configuration d'OnCommand Unified Manager», à la page 547
   - «Paramètres de configuration d'OnCommand API Service», à la page 548
4. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for NetApp Storage**, puis sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent NetApp Storage en mode silencieux, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier `netapp_storage_silent_config.txt` disponible à l'emplacement suivant :
   - Linux *rép_install*`/samples/netapp_storage_silent_config.txt`
     Exemple : `/opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt`
   - Windows *rép_install*`\samples\netapp_storage_silent_config.txt`
     Exemple : `C:\IBM\APM\samples\netapp_storage_silent_config.txt`
2. Dans le fichier `netapp_storage_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.
   Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données», à la page 546
   - «Paramètres de configuration d'OnCommand Unified Manager», à la page 547
   - «Paramètres de configuration d'OnCommand API Service», à la page 548
3. Sauvegardez et fermez le fichier `netapp_storage_silent_config.txt` et exécutez la commande suivante :
   - Linux *rép_install*`/bin/netapp_storage-agent.sh config` *nom_instance* *rép_install*`/samples/netapp_storage_silent_config.txt`
     Exemple : **`/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config nom_instance /opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt`**
   - Windows *rép_install*`\bin\netapp_storage-agent.bat config` *rép_install_nom_instance*`\samples\netapp_storage_silent_config.txt`
     Exemple : **`C:\IBM\APM\bin\netapp_storage-agent.bat config nom_instance C:\IBM\APM\samples\netapp_storage_silent_config.txt`**
     Où

     nom_instance
     Nom à attribuer à l'instance.

     rép_install
     Chemin d'installation de l'agent.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*`/bin/netapp_storage-agent.sh start` *nom_instance*
     Exemple : **`/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start nom_instance`**
   - Windows *rép_install*`\bin\netapp_storage-agent.bat start` *nom_instance*
     Exemple : **`C:\IBM\APM\bin\netapp_storage-agent.bat start nom_instance`**

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en répondant à des invites

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Sur la ligne de commande, entrez la commande suivante :

   rép_install/bin/netapp_storage-agent.sh config *nom_instance* Exemple : **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config nom_instance**

   Où

   nom_instance
   Nom à attribuer à l'instance.

   rép_install
   Chemin d'installation de l'agent.
2. Répondez aux invites en vous référant aux rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données»
   - «Paramètres de configuration d'OnCommand Unified Manager», à la page 547
   - «Paramètres de configuration d'OnCommand API Service», à la page 548
3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/netapp_storage-agent.sh start *nom_instance*

   Exemple : **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start nom_instance**

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration du fournisseur de données

Lorsque vous configurez l'agent NetApp Storage, vous pouvez modifier les valeurs par défaut des paramètres pour le fournisseur de données, comme le nombre maximal de fichiers journaux du fournisseur de données, la taille maximale du fichier journal et le niveau de détail inclus.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du fournisseur de données.

Tableau 145. Noms et descriptions des paramètres de configuration du fournisseur de données

Nom du paramètre	Description	Zone obligatoire
Nom d'instance (**KNU_INSTANCE_NAME**)	Nom de l'instance. **Restriction :** La zone Nom d'instance contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.	Oui
Maximum number of Data Provider Log Files (**KNU_LOG_FILE_MAX_COUNT**)	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui

Tableau 145. Noms et descriptions des paramètres de configuration du fournisseur de données (suite)

Nom du paramètre	Description	Zone obligatoire
Maximum Size in KB of Each Data Provider Log (**KNU_LOG_FILE_MAX_SIZE**)	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Level of Detail in Data Provider Log (**KNU_LOG_LEVEL**)	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 (Off) : aucun message n'est consigné. • 2 (Severe) : seules les erreurs sont consignées. • 3 (Warning) : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 (Info) : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 (Fine) : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 (Finer) : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information très détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 (Finest) : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Cette option risque d'affecter les performances de l'agent de surveillance de manière négative. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 (All) : toutes les erreurs et tous les messages sont consignés.	Oui

Paramètres de configuration d'OnCommand Unified Manager

Lorsque vous configurez l'agent NetApp Storage, vous pouvez modifier les valeurs par défaut des paramètres d'OnCommand Unified Manager (OCUM), tels que l'adresse IP du serveur OCUM, le nom d'utilisateur et le mot de passe.

Le tableau ci-après contient une description détaillée des paramètres de configuration de la source de données.

Tableau 146. Noms et descriptions des paramètres de configuration d'OnCommand Unified Manager

Nom du paramètre	Description	Zone obligatoire
Serveur (**KNU_DATASOURCE_HOST_ADDRESS**)	Nom d'hôte ou adresse IP du serveur NetApp OCUM à surveiller.	Oui

Tableau 146. Noms et descriptions des paramètres de configuration d'OnCommand Unified Manager (suite)

Nom du paramètre	Description	Zone obligatoire
Utilisateur (**KNU_DATASOURCE_USERNAME**)	Nom d'utilisateur sur le serveur NetApp OCUM dotés de privilèges lui permettant de collecter des données. La valeur par défaut est admin.	Oui
Mot de passe (**KNU_DATASOURCE_PASSWORD**)	Mot de passe de l'utilisateur que vous spécifiez dans le paramètre **Utilisateur**.	Oui
Confirmer le mot de passe	Mot de passe que vous avez indiqué dans le paramètre **Mot de passe**.	Oui
Protocole (**KNU_DATASOURCE_PROTOCOL**)	Protocole utilisé pour communiquer avec le serveur NetApp OCUM. La valeur par défaut est HTTPS.	Oui

Paramètres de configuration d'OnCommand API Service

Lorsque vous configurez l'agent NetApp Storage, vous pouvez modifier les valeurs par défaut des paramètres d'OnCommand API Service, tels que l'adresse hôte, le nom d'utilisateur et le mot de passe.

Le tableau ci-après contient une description détaillée des paramètres de configuration de la source de données.

Tableau 147. Noms et descriptions des paramètres de configuration d'OnCommand API Service

Nom du paramètre	Description	Zone obligatoire
Adresse hôte (**KNU_API_SERVICES_HOST_ADDRESS**)	Nom d'hôte ou adresse IP d'OnCommand API service.	Oui
Utilisateur (**KNU_API_SERVICES_USERNAME**)	Nom d'utilisateur disposant des privilèges lui permettant de se connecter à OnCommand API Service. La valeur par défaut est admin.	Oui
Mot de passe (**KNU_API_SERVICES_PASSWORD**)	Mot de passe de l'utilisateur que vous spécifiez dans le paramètre **Utilisateur**.	
Confirmer le mot de passe	Mot de passe que vous avez indiqué dans le paramètre **Mot de passe**.	Oui

Configuration de la surveillance de Node.js

Vous pouvez utiliser l'agent Node.js ou le collecteur de données Node.js autonome pour surveiller vos applications Node.js.

Avant de commencer

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent ou du collecteur de données. Pour accéder à la documentation des versions d'agent antérieures, voir tableau 148.

Tableau 148. Versions d'agent

Version d'agent	Documentation
01.00.13.00	IBM Performance Management 8.1.4
01.00.10.00	IBM Performance Management 8.1.3
01.00.09.00	IBM Performance Management 8.1.2
01.00.08.00	IBM Performance Management 8.1.1

Assurez-vous que votre environnement possède la configuration système requise pour l'Agent Node.js. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Node.js.

Pourquoi et quand exécuter cette tâche

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'Monitoring Agent for Node.js et le collecteur de données Node.js autonome.

- Pour surveiller les applications sur site, vous pouvez configurer le collecteur de données Node.js autonome ou l'Agent Node.js. Si vous souhaitez activer le suivi des transactions pour vos applications Node.js, configurez le collecteur de données autonome.
- Pour surveiller les applications IBM Cloud, configurez le collecteur de données Node.js. Pour plus d'informations sur le choix à faire entre le Agent Node.js et le collecteur de données Node.js autonome, voir «Agents et collecteurs de données», à la page 40.

Effectuez les étapes ci-après en fonction de vos besoins.

Procédure

- Configurez le Agent Node.js pour surveiller vos applications sur site.
  1. Ajoutez un collecteur de données d'agent à vos applications Node.js pour que l'agent fonctionne correctement. Voir «Configuration de l'Agent Node.js».
  2. Facultatif : Pour modifier le comportement de surveillance de votre agent, voir Configuration du collecteur de données de l'Agent Node.js.
  3. Facultatif : Pour configurer la collecte et l'affichage des données de diagnostic, voir Configuration du collecteur de données de diagnostic.
- Configurez le collecteur de données Node.js autonome pour surveiller les applications IBM Cloud.
  1. Pour configurer le collecteur de données Node.js autonome, voir «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 555.
  2. Pour modifier le comportement du collecteur de données Node.js autonome, voir «Personnalisation du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 556.
- Configurez le collecteur de données Node.js autonome pour surveiller les applications sur site.
  1. Pour configurer le collecteur de données Node.js autonome, voir «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 561.
  2. Pour modifier le comportement du collecteur de données Node.js autonome, voir «Personnalisation du collecteur de données Node.js pour les applications sur site», à la page 563.

Configuration de l'Agent Node.js

Vous devez ajouter un collecteur de données d'agent à votre application Node.js et la redémarrer pour que l'agent puisse commencer à la surveiller.

Avant de commencer

Avant de reconfigurer les paramètres de l'agent dans la même version, nettoyez les fichiers du collecteur de données qui ont été créés par la configuration précédente de la manière suivante :

1. Accédez au répertoire *rép_install*`/lx8266/nj/bin`.
2. Exécutez la commande `./uninstall.sh` pour supprimer les fichiers du collecteur de données existants.

Pourquoi et quand exécuter cette tâche

L'agent Node.js est un agent à instance unique. Il enregistre des sous-noeuds pour chaque application Node.js surveillée. Le sous-noeud possède la structure suivante :

```
NJ:hostname_port:NJA
```

Conseil : Si une application Node.js est en mode écoute sur plusieurs numéros de port, le numéro de port le plus bas est utilisé.

Vous devez ajouter un collecteur de données d'agent à votre application Node.js et la redémarrer pour que l'agent puisse commencer à la surveiller. Les collecteurs de données d'agent collectent des données qui sont transmises à l'agent Node.js. Actuellement, les collecteurs de données d'agent suivants sont fournis :

- Le collecteur de données de ressources collecte les données de surveillance des ressources à partir de vos applications Node.js.
- Le collecteur de données de diagnostic collecte les données de diagnostic et de surveillance des ressources à partir de vos applications Node.js.
- Le collecteur de données de trace de méthode collecte les traces de méthode, les données de diagnostic et les données de surveillance des ressources à partir de vos applications Node.js.

Procédure

1. Assurez-vous que l'ID utilisateur utilisé pour exécuter le serveur d'applications a des droits complets sur le répertoire `rép_install` de l'agent.
2. Accédez au répertoire *`rép_install`*`/bin` et exécutez la commande suivante :
   ```
   ./nodejs-agent.sh config
   ```
3. Suivez les instructions des invites pour spécifier les valeurs des options de configuration suivantes :

   KNJ_NODEJS_RUNTIME_BIN_LOCATION
   Répertoire contenant le dossier `bin` de votre exécution Node.js. Le répertoire par défaut est `/usr/local/bin`.

   KNJ_NPM_RUNTIME_BIN_LOCATION
   Répertoire contenant le dossier `bin` de votre commande **npm**. Le répertoire par défaut est `/usr/local/bin`.

   KNJ_NPM_LIB_LOCATION
   Répertoire contenant le dossier `lib` de votre répertoire d'installation global du package npm. Le répertoire par défaut est `/usr/local/lib`. Par exemple, si vous installez le package npm en exécutant la commande `npm install -g`, le package est installé dans */rép_base_nodejs*`/lib/node_modules` et **KNJ_NPM_LIB_LOCATION** correspond à */rép_base_nodejs*`/lib`.

   CP_PORT
   Port sur lequel l'agent écoute les données provenant des clients du socket. La valeur `0` indique qu'un port éphémère sera utilisé. La valeur par défaut est `63336`.

   Remarque : N'utilisez pas le numéro de port déjà utilisé sur votre système. Pour vérifier si le port est déjà utilisé, exécutez la commande `netstat -apn | grep` *`numéro_port`*.
4. Démarrez l'agent en exécutant la commande suivante :
   ```
   ./nodejs-agent.sh start
   ```
5. Vérifiez que l'Agent Node.js est démarré avec succès. Le dossier *`KNJ_NPM_LIB_LOCATION`*`/node_modules/ibmapm` est généré si l'agent démarre correctement.
6. En fonction de l'offre dont vous disposez et des exigences, insérez l'une des entrées suivantes dans le fichier `.js` de votre application Node.js pour configurer les collecteurs de données d'agent :

   Remarque : Une seule entrée peut être ajoutée à votre application Node.js afin d'activer les fonctionnalités du collecteur de données de l'agent. De même, si vous activez les fonctionnalités qui ne sont pas incluses dans l'offre, le système peut être inutilement surchargé, ce qui peut réduire l'efficacité de l'exécution de l'application.

- Si vous n'avez que des fonctionnalités de surveillance de ressources, vous pouvez ajouter le collecteur de données de ressource. Pour ce faire, insérez la ligne suivante au début du fichier d'application Node.js :

  ```
  require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
  ```

  Si la valeur de **KNJ_NPM_LIB_LOCATION** est /usr/local/lib dans votre environnement, la ligne apparaît comme suit :

  ```
  require('/usr/local/lib/node_modules/ibmapm');
  ```

- Si vous avez des fonctionnalités de diagnostic en plus de la surveillance au niveau de la ressource, vous pouvez choisir d'ajouter l'un des collecteurs de données d'agent suivants :
  - Pour ajouter le collecteur de données de trace de méthode, insérez la ligne suivante au début du fichier d'application Node.js :

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/methodtrace.js');
    ```

  - Pour ajouter le collecteur de données de diagnostic, insérez la ligne suivante au début du fichier d'application Node.js :

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/deepdive.js');
    ```

  - Pour ajouter le collecteur de données de surveillance des ressources, insérez la ligne suivante au début du fichier d'application Node.js :

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
    ```

  Pour améliorer les performances, ajoutez le collecteur de données de trace de méthode à des fins de débogage uniquement.

Remarque : le code des plug-in change à partir de Cloud APM, Privateversion 8.1.4. Si vous mettez à niveau votre agent à partir de versions antérieures, vous devez mettre à jour le code des collecteurs de données existants dans vos applications pour que la fonctionnalité de surveillance fonctionne correctement.

7. Redémarrez l'application Node.js pour activer le collecteur de données de l'agent.

Résultats

Vous avez correctement configuré l'Agent Node.js.

Que faire ensuite

- Vous pouvez à présent vérifier que les données de l'Agent Node.js s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

  Important : pour ajouter votre application à la console Cloud APM, choisissez **Node.js** dans l'éditeur d'application.

- Vous pouvez modifier le comportement d'exécution des collecteurs de données d'agent Node.js. Pour plus d'informations, voir Configuration du collecteur de données de l'agent Node.js.
- Vous pouvez activer la collecte et l'affichage des données de diagnostic en configurant le collecteur de données de diagnostic. Pour plus d'informations, voir Configuration du collecteur de données de diagnostic.

Configuration du collecteur de données de l'Agent Node.js

Vous pouvez modifier le comportement du collecteur de données de chaque agent Node.js en changeant la configuration d'environnement d'exécution qui lui est associée dans son fichier de configuration.

Fichier de configuration de l'environnement d'exécution

Le code du collecteur de données Node.js se trouve dans le répertoire suivant :

KNJ_NPM_LIB_LOCATION/node_modules/ibmapm

où *KNJ_NPM_LIB_LOCATION* correspond au répertoire du dossier lib de votre répertoire d'installation global du package npm. Le répertoire par défaut est /usr/local/lib.

Il existe également un fichier de configuration d'environnement d'exécution pour le collecteur de données de chaque agent dans le même dossier. Le collecteur de données de l'agent lit le fichier de configuration toutes les minutes.

Conseil : Le fichier de configuration d'environnement d'exécution est nommé comme suit :

plugin_*numéro de port d'application*_conf.json

Lorsque vous modifiez le contenu du fichier de configuration, le comportement du collecteur de données de l'agent associé change. Le fichier de configuration contient deux types d'information que vous pouvez modifier :

- Règles de filtrage d'URL
- Paramètres de consignation du collecteur de données de l'agent

Règles de filtrage d'URL

Vous pouvez modifier les règles de filtrage d'URL dans le fichier de configuration d'exécution. Expressions régulières qui sont utilisées pour mapper le nom de chemin d'URL à un nom de chemin personnalisé par l'utilisateur. Vous pouvez mapper l'URL à un nom de chemin personnalisé pour répondre aux exigences suivantes :

- Agrégation d'URL avec des chemins similaires. Prenons l'exemple des chemins d'URL suivants :

  ```
  /demo/poll/1
  /demo/poll/2
  /demo/poll/3
  ...
  ```

  Sur le serveur Web, les demandes associées à ces chemins sont probablement exécutées par une routine commune ; vous pouvez donc agréger les chemins en un type d'URL unique en utilisant le filtre de l'exemple ci-dessous.

  ```
  "filters":
  [
   {
    "pattern": "/demo/poll/.+",
    "to": "/demo/poll/"
   }
  ```

  Avec ce filtre, toutes les demandes vers des chemins d'URL semblables à "/demo/poll/xxx" sont mappées au type de chemin d'URL "/demo/poll". La moyenne des temps de réponse pour toutes les demandes vers les chemins d'URL de ce type est alors calculée pour générer une valeur unique. Une telle agrégation permet d'utiliser plus efficacement les ressources disponibles.
- Omission des chemins d'URL pointant vers des fichiers statiques ou filtrage de certains types de demande. Par exemple, si une page Web inclut des images qui génèrent des demandes de téléchargement sur des serveurs distincts, l'affichage des temps de réponse pour ces types de demandes peut ne pas présenter d'intérêt.

  Pour filtrer un type de demande, ne définissez pas la valeur "to", conformément au format de l'exemple suivant :

```
"filters":
[
 {
  "pattern": "GET /css/.+\\.css$",
  "to": ""
 }
```

Lors de l'exécution de ce filtre, le fichier `.css` concerné par la demande est ignoré. Par conséquent, vous pouvez utiliser les ressources disponibles de manière plus efficace sur les demandes que vous devez surveiller.

Dans le fichier de configuration, les règles de filtrage d'URL sont répertoriées dans un tableau JSON nommé `filters` :

```
"filters":
[
    {
        "pattern": ".+\\.png$",
        "to": ""
    },
    {
        "pattern": ".+\\.jpg$",
        "to": ""
    },
    {
        "pattern": "GET /js/.+\\.js$",
        "to": ""
    },
    {
        "pattern": "GET /css/.+\\.css$",
        "to": ""
    }
]
```

Chaque membre du tableau est une règle de filtrage. Lorsqu'une demande HTTP est reçue par le collecteur de données de l'agent, celui-ci extrait le nom de chemin d'URL de la demande et le compare à chaque `"pattern"`. Si le nom de chemin ne correspond à aucun `"pattern"`, le nom de chemin d'URL d'origine est conservé et utilisé pour les mesures.

Paramètre de consignation du collecteur de données de l'agent

Vous pouvez modifier les comportements de consignation en modifiant le paramètre dans le fichier de configuration `config.properties` du répertoire *KNJ_NPM_LIB_LOCATION*`/node_modules/ibmapm/etc`. Le paramètre de consignation suivant est fourni et peut être modifié :

Niveau de consignation

Dans le fichier de configuration, l'entrée correspondant au niveau de consignation est `KNJ_LOG_LEVEL=info`, ce qui signifie que les informations récapitulatives sur les actions sont sauvegardées dans le journal. Vous pouvez définir le niveau de consignation en modifiant la valeur de `KNJ_LOG_LEVEL`. La valeur par défaut est `info` et le journal est imprimé dans la sortie standard.

Les cinq valeurs de niveau de consignation suivantes sont prises en charge :

off Les journaux ne sont pas imprimés.

error Les informations ne sont consignées qu'en cas d'erreur.

info Les informations sont consignées lorsque le collecteur de données Agent Node.js s'exécute normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées.

debug Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur.

all Toutes les informations sont consignées dans le journal.

Configuration du collecteur de données de diagnostic de l'Agent Node.js

La prise en charge de la collecte des données de diagnostic est désactivée par défaut. Si vous avez des fonctionnalités de diagnostic, vous devez définir et ajuster la collecte de données pour les applications Node.js.

Procédure

- Pour modifier les paramètres du collecteur de données pour une application spécifique en cours d'exécution :
  1. Accédez au répertoire *KNJ_NPM_LIB_LOCATION*/node_modules/ibmapm et ouvrez le fichier plugin_*port*_conf.json dans un éditeur de texte.

     Conseil : Pour plus d'informations sur *KNJ_NPM_LIB_LOCATION*, voir la description du paramètre «KNJ_NPM_LIB_LOCATION», à la page 550
  2. Utilisez le tableau suivant pour obtenir des informations sur la modification des paramètres du collecteur de données :

Tableau 149. Paramètres du collecteur de données

Catégorie de données de diagnostic	Description	Propriété	Action
Retardement minimum pour la génération d rapport de trace de pile	Indique le seuil de temps de réponse pour la collecte de la trace de pile d'une demande ou d'un appel de méthode. Si le temps de réponse d'une demande ou d'un appel de méthode dépasse cette valeur, le collecteur de données collecte sa trace de pile.	minClockStack	Valeur en millisecondes
Retardement minimum de signalement des demandes	Indique le seuil de temps de réponse pour la collecte de la trace de méthode d'une instance de demande. Si le temps de réponse d'une instance de demande dépasse ce seuil, le collecteur de données collecte sa trace de méthode.	minClockTrace	Valeur en millisecondes
Nombre maximum d'événements par fichier	Indique le nombre maximal d'événements à sauvegarder dans un fichier .jso. Le fichier .jso enregistre les données de diagnostic de ces événements.	eventsPerFile	Nombre maximum d'événements
Délai de signalement maximum dans un fichier	Indique la durée maximale d'enregistrement des données de diagnostic par le fichier .jso	fileCommitTime	Délai maximum en secondes

Tableau 149. Paramètres du collecteur de données (suite)

Catégorie de données de diagnostic	Description	Propriété	Action
Nombre maximum de fichiers à conserver avant de supprimer les plus anciens	Indique le nombre maximal de fichiers `.jso` à conserver avant que les anciens fichiers soient supprimés.	`maxFiles`	Nombre maximum de fichiers
Période d'échantillonnage des demandes	Indique la période d'échantillonnage des demandes.	`sampling`	Période d'échantillonnage considérée. La valeur par défaut est `10`. La valeur `10` indique que l'agent collecte une demande sur 10.

- Facultatif : Définissez la variable d'environnement *SECURITY_OFF* si vous voulez que le collecteur de données de diagnostic collecte les informations sensibles de l'utilisateur, telles que les cookies, les contextes de demande HTTP et les contextes de requête de base de données. Ces informations ne sont pas collectées par défaut. Soyez prudent lorsque vous définissez cette variable, car le processus peut entraîner une fuite des informations.

  Linux Par exemple, pour définir cette variable d'environnement, exécutez la commande suivante :

  ```
  export SECURITY_OFF=true
  ```

Résultats

La configuration du collecteur de données de diagnostic est modifiée pour l'application en cours d'exécution que vous avez spécifiée ou pour toutes les applications.

Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud

Pour collecter des informations concernant les applications Node.js sur IBM Cloud, vous devez configurer le collecteur de données Node.js autonome.

Avant de commencer

1. Assurez-vous que votre application Node.js peut s'exécuter avec succès localement. Le collecteur de données Node.js autonome peut surveiller Node.js version 4.0.0 et groupes de correctifs à venir, et version 6.0.0 et groupes de correctifs à venir.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Configurez le package du collecteur de données avec les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `nodejs_datacollector_8.1.4.0.5.tgz` est inclus dans le répertoire extrait.
2. Extrayez le fichier `nodejs_datacollector_8.1.4.0.5.tgz`, par exemple, en exécutant la commande suivante :

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.5.tgz
   ```
3. Extrayez le fichier `ibmapm.tgz` dans le dossier `nodejs_dc` en exécutant la commande suivante :

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Vous obtiendrez un dossier `ibmapm`.
4. Copiez le dossier `ibmapm` qui est extrait du module de collecteur de données dans le répertoire de base de votre application, par exemple, en exécutant la commande suivante :

```
cp –r répertoire_accès_au_dossier_ibmapm  répertoire_base_de_votre_application_Node.js
```

Conseil : Le répertoire de base de votre application Node.js est déterminé par la commande que vous utilisez pour démarrer l'application Node.js et par le répertoire qui contient votre fichier principal. Si vous utilisez la commande **node app.js** pour démarrer votre application Node.js et si le fichier principal `app.js` se trouve dans le répertoire `/root/nodejs_app`, `/root/nodejs_app` est le répertoire de base de votre application.

5. Dans le fichier `package.json` de votre application Node.js, ajoutez les lignes suivantes dans la section Dépendances :

```
"appmetrics": "^3.0.1",
"kubernetes-client": "^3.16.0",
"properties": "^1.2.1",
"uuid":"^2.0.2",
"log4js": "^0.6.38",
"https-proxy-agent":"^1.0.0",
"agent-base": "^2",
"debug": "^2",
"extend": "^3",
"request": "^2.72.0"
```

A faire : veillez à inclure la virgule à la fin de chaque ligne du fichier, à l'exception de la dernière, et conservez la syntaxe correcte du fichier `package.json`.

6. Ajoutez la ligne suivante au début du fichier principal de l'application Node.js :

```
require('./ibmapm');
```

Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.

7. A partir du répertoire qui contient le fichier `manifest.yml` de votre application Node.js, connectez-vous à IBM Cloud puis exécutez la commande suivante :

```
cf push
```

Conseil : Pour un fichier `manifest.yml` exemple, voir «Exemple de fichier `manifest.yml`», à la page 237.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez vérifier que les données de surveillance de votre application IBM Cloud sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

A faire : Pour ajouter votre application à la console Cloud APM, choisissez **Node.js Runtime** dans l'éditeur d'application.

Personnalisation du collecteur de données Node.js autonome pour les applications IBM Cloud

Vous pouvez ajouter des variables d'environnement dans l'interface utilisateur IBM Cloud pour personnaliser la surveillance de votre application IBM Cloud.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Node.js

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance Node.js sur IBM Cloud.

Tableau 150. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• `https://`*IP ou nom d'hôte du serveur*`:443` • `http://`*IP ou nom d'hôte du serveur*`:80`	L'URL de la passerelle de serveur cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n` *mot de passe du fichier de clés* `| base64` pour chiffrer votre mot de passe. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	`http://`*serveur HTTP hébergé*`:`*port*`/keyfile.p12`	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_SNI	Facultative	`owner host` dans votre fichier de clés	L'hôte propriétaire dans votre fichier de clés. La valeur par défaut est `default.server`, c'est-à-dire l'hôte propriétaire indiqué dans le fichier de clés par défaut qui est fourni dans le répertoire d'installation du serveur Cloud APM. Si vous n'utilisez pas le fichier de clés par défaut, ouvrez le fichier de clés que vous utilisez et recherchez `owner`. Définissez la variable sur la même valeur que pour `owner`. Si vous ne définissez pas cette variable, `default.server` est la valeur par défaut qui est utilisée.

Tableau 150. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_SAMPLING	Facultative	Nombre des demandes par échantillonnage	Le nombre de demandes sur la base duquel un échantillon est prélevé. La valeur par défaut est `10`, ce qui signifie qu'une demande sur 10 est surveillée. Si vous ne définissez pas cette variable, la valeur par défaut `10` est utilisée.
KNJ_MIN_CLOCK_TRACE	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. La valeur par défaut est `0`. Si vous ne définissez pas cette variable, la valeur par défaut `0` est utilisée.
KNJ_MIN_CLOCK_STACK	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. La valeur par défaut est `0`. Si vous ne définissez pas cette variable, la valeur par défaut `0` est utilisée.
KNJ_DISABLE_METHODTRACE	Facultative	• `True` • `False`	Active ou désactive la trace de méthode. • Si vous définissez cette variable sur true, la trace de méthode pour les demandes est désactivée. • Si vous définissez cette valeur sur false, la trace de méthode pour les demandes est activée. Il s'agit de la valeur par défaut. Si vous ne définissez pas cette variable, la valeur par défaut `False` est utilisée et la trace de méthode pour les demandes est activée.

Tableau 150. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_ENABLE_TT	Facultative	• `true` • `false`	Active ou désactive le suivi des transactions d'AAR. • Si vous définissez cette variable sur true, le suivi des transactions d'AAR est activé. • Si vous définissez cette variable sur false, le suivi des transactions d'AAR est désactivé. Par défaut, cette valeur n'est pas définie, ce qui signifie que le suivi des transactions est désactivé.
KNJ_AAR_BATCH_FREQ	Facultative	Intervalle d'envoi des données AAR, en secondes	Indique l'intervalle auquel les données AAR sont envoyées par lot au serveur, en secondes. La valeur par défaut est de 60, ce qui signifie que les données AAR sont envoyées par lot au serveur toutes les minutes. **Remarque :** cette variable fonctionne avec KNJ_AAR_BATCH_COUNT pour déterminer quand les données AAR sont envoyées par lot au serveur. Si la condition définie par l'une des deux variables est remplie, les données AAR sont envoyées par lot. Si les demandes contenues dans les données AAR atteignent leur nombre maximal, par exemple 100, dans un délai plus court que celui défini, les données sont tout de même envoyées immédiatement par lot.
KNJ_AAR_BATCH_COUNT	Facultative	Nombre maximal de demandes pouvant être contenues dans un lot de données AAR	Indique le nombre maximal de demandes pouvant être contenues dans un lot de données AAR avant que ce lot ne soit envoyé au serveur. La valeur par défaut est de 100, ce qui signifie que lorsque le nombre de demandes pouvant être contenues dans un lot de données AAR atteint 100, ce lot de données AAR est envoyé au serveur.

Tableau 150. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_LOG_LEVEL	Facultative	Niveau d'information imprimé dans le journal	Contrôle le niveau d'information imprimé dans le journal. Les niveaux suivants sont fournis : **off** Les journaux ne sont pas imprimés. **error** Les informations ne sont consignées qu'en cas d'erreur. **info** Les informations sont consignées lorsque le collecteur de données d'agent Node.js s'exécute normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées. **debug** Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur. **all** Toutes les informations sont consignées dans le journal. Par défaut, le niveau de consignation est `info`, ce qui signifie que les informations récapitulatives sur les actions du collecteur de données sont imprimées dans le journal. Les journaux sont imprimés dans la sortie standard.
SECURITY_OFF	Facultative	• `true` • `false`	Active ou désactive la collecte des informations sensibles de l'utilisateur, telles que les cookies, le contexte de demande HTTP et le contexte de requête de base de données. • Si vous définissez cette variable sur true, les informations sensibles de l'utilisateur sont collectées. • Si vous définissez cette variable sur false, les informations sensibles de l'utilisateur ne sont pas collectées. Il s'agit de la valeur par défaut. Si vous ne spécifiez pas cette variable, la valeur par défaut `false` est utilisée et les informations sensibles de l'utilisateur ne sont pas collectées.

Annulation de la configuration du collecteur de données Node.js autonome pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller votre environnement Node.js ou si vous souhaitez mettre à niveau le collecteur de données Node.js autonome, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Node.js autonome.

Procédure

1. Supprimez la ligne `require('./ibmapm');` du fichier principal de l'application.

   Conseil : Si vous démarrez votre application en exécutant la commande **`node app.js`**, `app.js` est le fichier principal de votre application.

2. Supprimez les dépendances suivantes du fichier `package.json`.

   ```
   "appmetrics": "^3.0.1",
   "properties": "^1.2.1",
   "uuid":"^2.0.2",
   "log4js": "^0.6.38",
   "https-proxy-agent":"^1.0.0",
   "agent-base": "^2",
   "debug": "^2",
   "extend": "^3",
   "request": "^2.72.0"
   ```

   A faire : Ne supprimez pas les dépendances dont votre application a besoin.

3. Supprimez le dossier `ibmapm` du répertoire de base de votre application.

Résultats

Vous avez correctement annulé la configuration du collecteur de données Node.js autonome.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Configuration du collecteur de données Node.js autonome pour les applications sur site

Pour collecter des informations sur votre application sur site Node.js, vous devez configurer le collecteur de données Node.js.

Avant de commencer

1. Assurez-vous que votre application Node.js peut s'exécuter avec succès localement. Le collecteur de données Node.js autonome peut surveiller Node.js version 4.0.0 et groupes de correctifs à venir, et version 6.0.0 et groupes de correctifs à venir.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Configurez le package du collecteur de données avec les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `nodejs_datacollector_8.1.4.0.5.tgz` est inclus dans le répertoire extrait.
2. Déterminez le répertoire de base de votre application.
   - Pour les applications Node.js type, si vous utilisez la commande **node app.js** pour démarrer votre application Node.js et que le fichier principal `app.js` se trouve dans le répertoire `/root/nodejs_app`, `/root/nodejs_app` est le répertoire de base de votre application.
   - Pour les membres de collectivité dans l'environnement IBM API Connect, exécutez la commande **wlpn-server list** pour afficher la liste de tous les membres de collectivité sur la même machine. Le répertoire de base de votre membre de collectivité est au format suivant :

     répertoire_utilisateur/*nom_membre-collectivité*/package

     Par exemple, si vous obtenez `/root/wlpn/rock-8345a96-148538-1/package` comme sortie de commande, `/root/wlpn` est le répertoire utilisateur et `rock-8345a96-148538-1` est le nom de membre de collectivité.
   - Pour les applications Developer Portal dans l'environnement IBM API Connect, vous pouvez exécuter la commande **ps -ef | grep node** pour rechercher le répertoire de base. Si vous obtenez la sortie de commande suivante, par exemple, le répertoire de base est `/home/admin/bgsync` et le fichier principal de votre application est `rest_server.js` :

     ```
     admin 19085 1 0 Jun25 ?  00:06:53 /usr/local/bin/node /home/admin/bgsync/rest_server.js
     ```
3. A partir du répertoire de base de votre application, exécutez la commande suivante pour extraire les fichiers du module de collecteur de données :

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.5.tgz
   ```
4. Exécutez la commande suivante pour installer le collecteur de données dans votre application :

   ```
   npm install nodejs_dc/ibmapm.tgz
   ```
5. Ajoutez la ligne suivante au début du fichier principal de l'application Node.js :

   ```
   require('ibmapm');
   ```
   - Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.
   - Pour les membres de collectivité dans l'environnement IBM API Connect, le fichier principal est défini dans le fichier `package.json` dans le répertoire de base ou ses sous-dossiers. Par défaut, le fichier principal est *répertoire_base*`/server/server.js`, où *répertoire_base* est le répertoire de base de votre membre de collectivité.
   - Pour les applications Developer Portal dans l'environnement IBM API Connect, vous pouvez exécuter la commande **ps -ef | grep node** pour rechercher le fichier principal. Si vous obtenez la sortie de commande suivante, par exemple, le fichier principal de votre application est `rest_server.js`.

     ```
     admin 19085 1 0 Jun25 ?  00:06:53 /usr/local/bin/node /home/admin/bgsync/rest_server.js
     ```
6. Redémarrez votre application.

   Conseil :
   - Pour redémarrer votre membre de collectivité, exécutez la commande `wlpn-server stop` *nom_membre_collectivité*. Le membre de collectivité redémarre automatiquement après l'exécution de cette commande. S'il ne démarre pas, exécutez la commande `wlpn-server start` *nom_membre_collectivité* pour le redémarrer manuellement.
   - Pour redémarrer vos applications Developer Portal, exécutez d'abord la commande `/etc/init.d/restservice stop` pour arrêter l'application, puis la commande `/etc/init.d/restservice start` pour la démarrer.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

- Vous pouvez vérifier que les données de surveillance de votre application s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.
- Pour afficher les informations de topologie pour votre environnement API Connect, activez le suivi des transactions. Pour plus d'instructions, consultez la description de la variable *KNJ_ENABLE_TT* dans «Personnalisation du collecteur de données Node.js pour les applications sur site».

A faire : Pour ajouter votre application à la console Cloud APM, choisissez **Node.js Runtime** dans l'éditeur d'application.

Personnalisation du collecteur de données Node.js pour les applications sur site

En modifiant des fichiers dans le module de collecteur de données, vous pouvez définir les variables d'environnement de façon à personnaliser la surveillance pour votre application Node.js.

Deux fichiers sont fournis pour personnaliser les paramètres du collecteur de données, `global.environment` et `config.properties`. Après avoir modifié les paramètres dans ces fichiers, redémarrez l'application Node.js pour que les modifications soient prises en compte.

En modifiant le fichier `global.environment`, vous pouvez personnaliser la connexion entre le collecteur de données et le serveur Cloud APM. Si vous voulez utiliser un autre serveur Cloud APM au lieu de la valeur par défaut, ou si le fichier de clés ou son mot de passe est modifié, modifiez les paramètres du fichier `global.environment` pour reconnecter le collecteur de données au serveur Cloud APM.

En modifiant le fichier `config.properties`, vous pouvez personnaliser le comportement du collecteur de données en fonction de vos besoins, par exemple, activer ou désactiver la trace de méthode.

Le fichier de configuration `global.environment`

Le tableau 151 indique les variables que vous pouvez définir dans le fichier de configuration `global.environment`, ainsi que leur description. Vous trouverez le fichier `global.environment` dans le dossier `ibmapm/etc` dans lequel votre collecteur de données Node.js est installé.

Tableau 151. Variables prises en charge dans le fichier `global.environment`

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https://*IP ou nom d'hôte du serveur*:443 • http://*IP ou nom d'hôte du serveur*:80	L'URL de la passerelle de serveur sur site cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n` *`mot de passe du fichier de clés`* `| base64` pour chiffrer votre mot de passe. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.

Tableau 151. Variables prises en charge dans le fichier `global.environment` (suite)

Nom de la variable	Importance	Valeur	Description
APM_KEYFILE_URL	Facultative	http://*serveur http hébergé*:*port*/keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_SNI	Facultative	`owner host` dans votre fichier de clés	L'hôte propriétaire dans votre fichier de clés. La valeur par défaut est `default.server`, c'est-à-dire l'hôte propriétaire indiqué dans le fichier de clés par défaut qui est fourni dans le répertoire d'installation du serveur Cloud APM. Si vous n'utilisez pas le fichier de clés par défaut, ouvrez le fichier de clés que vous utilisez et recherchez `owner`. Définissez la variable sur la même valeur que pour `owner`. Si vous ne définissez pas cette variable, `default.server` est la valeur par défaut qui est utilisée.

Le fichier `config.properties`

Le tableau 152 indique les variables d'environnement que vous pouvez définir dans le fichier de configuration `config.properties`, ainsi que leur description. Vous trouverez le fichier `config.properties` dans le dossier `ibmapm/etc` dans lequel votre collecteur de données Node.js est installé.

Tableau 152. Variables prises en charge dans le fichier `config.properties`

Nom de la variable	Importance	Valeur	Description
KNJ_SAMPLING	Facultative	Nombre des demandes par échantillonnage	Le nombre de demandes sur la base duquel un échantillon est prélevé. La valeur par défaut est `10`, ce qui signifie qu'une demande sur 10 est surveillée. Si vous ne définissez pas cette variable, la valeur par défaut `10` est utilisée.
KNJ_MIN_CLOCK_TRACE	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. La valeur par défaut est `1`. Si vous ne définissez pas cette variable, la valeur par défaut `1` est utilisée.

Tableau 152. Variables prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_MIN_CLOCK_STACK	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. La valeur par défaut est `100`. Si vous ne définissez pas cette variable, la valeur par défaut `100` est utilisée.
KNJ_DISABLE_METHODTRACE	Facultative	• True • False	Active ou désactive la trace de méthode. • Si vous définissez cette variable sur true, la trace de méthode pour les demandes est désactivée. • Si vous définissez cette valeur sur false, la trace de méthode pour les demandes est activée. Il s'agit de la valeur par défaut. Si vous ne définissez pas cette variable, la valeur par défaut `False` est utilisée et la trace de méthode pour les demandes est activée.
KNJ_ENABLE_TT	Facultative	• True • False	Active ou désactive le suivi des transactions d'AAR. • Si vous définissez cette variable sur true, le suivi des transactions d'AAR est activé. • Si vous définissez cette variable sur false, le suivi des transactions d'AAR est désactivé. Par défaut, cette valeur n'est pas définie, ce qui signifie que le suivi des transactions est désactivé.
KNJ_AAR_BATCH_FREQ	Facultative	Intervalle d'envoi des données AAR, en secondes	Indique l'intervalle auquel les données AAR sont envoyées par lot au serveur, en secondes. La valeur par défaut est de 60, ce qui signifie que les données AAR sont envoyées par lot au serveur toutes les minutes. **Remarque :** Cette variable fonctionne avec KNJ_AAR_BATCH_COUNT pour déterminer quand les données AAR sont envoyées par lot au serveur. Si la condition définie par l'une des deux variables est remplie, les données AAR sont envoyées par lot. Si les demandes contenues dans les données AAR atteignent leur nombre maximal, par exemple 100, dans un délai plus court que celui défini, les données sont tout de même envoyées immédiatement par lot.

Tableau 152. Variables prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_AAR_BATCH_COUNT	Facultative	Nombre maximal de demandes pouvant être contenues dans un lot de données AAR	Indique le nombre maximal de demandes pouvant être contenues dans un lot de données AAR avant que ce lot ne soit envoyé au serveur. La valeur par défaut est de 100, ce qui signifie que lorsque le nombre de demandes pouvant être contenues dans un lot de données AAR atteint 100, ce lot de données AAR est envoyé au serveur.
KNJ_LOG_LEVEL	Facultative	Niveau d'information imprimé dans le journal	Contrôle le niveau d'information imprimé dans le journal. Les niveaux suivants sont fournis : **off** Les journaux ne sont pas imprimés. **error** Les informations ne sont consignées qu'en cas d'erreur. **info** Les informations sont consignées lorsque le collecteur de données d'agent Node.js s'exécute normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées. **debug** Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur. **all** Toutes les informations sont consignées dans le journal. Par défaut, le niveau de consignation est `info`, ce qui signifie que les informations récapitulatives sur les actions du collecteur de données sont imprimées dans le journal. Les journaux sont imprimés dans la sortie standard.

Tableau 152. Variables prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
SECURITY_OFF	Facultative	• `true` • `false`	Active ou désactive la collecte des informations sensibles de l'utilisateur, telles que les cookies, le contexte de demande HTTP et le contexte de requête de base de données. • Si vous définissez cette variable sur true, les informations sensibles de l'utilisateur sont collectées. • Si vous définissez cette variable sur false, les informations sensibles de l'utilisateur ne sont pas collectées. Il s'agit de la valeur par défaut. Si vous ne spécifiez pas cette variable, la valeur par défaut `false` est utilisée et les informations sensibles de l'utilisateur ne sont pas collectées.

Annulation de la configuration du collecteur de données Node.js autonome pour les applications sur site

Si vous n'avez pas besoin de surveiller votre environnement Node.js ou si vous souhaitez mettre à niveau le collecteur de données Node.js autonome, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Node.js autonome.

Procédure

1. Supprimez la ligne `require('./ibmapm');` du fichier principal de l'application.

   Conseil : Si vous démarrez votre application en exécutant la commande **`node app.js`**, `app.js` est le fichier principal de votre application.
2. Supprimez `"ibmapm":"^1.0.0"` de la section de dépendances dans le fichier `package.json` de votre application Node.js.
3. Supprimez le dossier `node_modules` du répertoire de base de votre application.
4. Exécutez la commande `npm install` pour installer les dépendances de l'application.

Résultats

Vous avez correctement annulé la configuration du collecteur de données Node.js autonome.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Configuration de la surveillance d'OpenStack

Vous devez configurer l'Monitoring Agent for OpenStack pour qu'il puisse surveiller automatiquement l'environnement de l'Agent OpenStack.

Procédure

1. Configurez l'agent en répondant aux invites. Pour plus d'informations, voir «Configuration de l'Agent OpenStack».
2. Si vous voulez collecter des informations sur le processus, configurez le collecteur de données de l'Agent OpenStack. Pour plus d'informations, voir «Activation de la collecte des informations liées aux processus et des connexions SSH», à la page 570.
3. Entrez les valeurs de configuration pour que l'agent fonctionne. Pour obtenir des instructions, voir «Ajout des valeurs de configuration», à la page 571.

Configuration de l'Agent OpenStack

Pour un environnement type, si vous souhaitez que l'Agent OpenStack surveille automatiquement l'environnement OpenStack, vous devez configurer l'agent au préalable.

Avant de commencer

Assurez-vous d'avoir installé tous les logiciels requis, comme décrit dans la rubrique Préinstallation sur des systèmes Linux.

Procédure

Vous avez deux options pour configurer l'Agent OpenStack sur un système Linux :

- Pour configurer l'agent en exécutant le script et en répondant aux invites, voir «Configuration interactive».
- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans interaction, voir «Configuration en mode silencieux», à la page 569.

Configuration interactive

Procédure

1. Pour configurer l'agent, exécutez la commande suivante :

   ```
   rép_install/bin/openstack-agent.sh config nom_instance
   ```

   où *rép_install* représente le répertoire d'installation de votre Agent OpenStack. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
2. Lorsque vous êtes invité à `entrer le nom d'instance`, spécifiez un nom d'instance.

   Important : L'Agent OpenStack est un agent à plusieurs instances et nécessite un nom d'instance pour chaque instance d'agent. Le nom d'instance que vous indiquez est inclus dans le nom de système géré `nom_instance:nom_hôte:sg`. La longueur du nom d'instance que vous indiquez est limitée à 28 caractères sans la longueur de votre nom d'hôte. Par exemple, si vous indiquez `OS1` comme nom d'instance, votre nom de système géré est `OS1:nom_hôte:SG`.
3. A l'invite `Edit Monitoring Agent for OpenStack`, appuyez sur `Entrée` pour continuer.
4. A l'invite `Edit OpenStack environment authentication information`, fournissez les informations suivantes :

   ```
   OpenStack authentication url (default is: http://localhost:identity/v3):
   OpenStack username (default is: admin):
   Enter OpenStack password (default is: ):
   Re-type: OpenStack password (default is: ):
   OpenStack tenant name (default is: admin):
   ```
5. Lorsque le programme vous demande l'`emplacement de l'exécutable Python`, indiquez cet emplacement, par exemple `/usr/bin/python`. Vous pouvez trouver le chemin complet en exécutant la commande suivante dans votre environnement :

   ```
   which python
   ```

6. Lorsque le programme vous demande le numéro de port, acceptez la valeur par défaut ou indiquez un numéro de port. Ce port sert à surveiller la communication interne entre le collecteur de données de l'Agent OpenStack et l'Agent OpenStack, qui sont installés seulement sur un serveur local. L'agent est en mode écoute sur ce port pour rechercher les données du collecteur de données. La valeur par défaut de 0 indique qu'un port éphémère est utilisé quand l'agent démarre. Sur un serveur avec des règles de sécurité strictes sur des ports, vous pouvez configurer un port spécifique pour que l'agent l'utilise. Ce port est réservé à l'usage interne par l'agent et n'est pas lié à l'environnement OpenStack.
7. Editez le fichier /etc/hosts sur votre système pour ajouter le mappage hôte de chaque noeud surveillé.

Configuration en mode silencieux

Procédure

1. Ouvrez le fichier sg_silent_config.txt dans un éditeur de texte. Ce fichier se trouve dans le répertoire *rép_install*/samples, où *rép_install* est le répertoire d'installation de l'Agent OpenStack.
2. Editez le fichier de configuration sg_silent_config.txt de l'Agent OpenStack.
3. Indiquez les valeurs des paramètres identifiés dans le fichier. Le fichier de réponses contient les commentaires qui définissent les paramètres disponibles et les valeurs à indiquer.
4. Sauvegardez le fichier et quittez l'application.
5. Editez le fichier /etc/hosts sur votre système pour ajouter le mappage hôte de chaque noeud surveillé.
6. A partir du répertoire *rép_install*/samples, exécutez la commande suivante pour configurer l'agent :

   rép_install/bin/openstack-agent.sh config *nom_instance chemin_fichier_réponses*

   où *rép_instance* est le nom de l'instance à configurer et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux. Définissez un chemin absolu vers ce fichier.

   Par exemple, si le fichier de réponses se trouve dans le répertoire par défaut, lancez la commande suivante.

   ```
   /opt/ibm/apm/agent/bin/openstack-agent.sh config nom_instance
   /opt/ibm/apm/agent/samples/sg_silent_config.txt
   ```

Résultats

L'agent est configuré.

Que faire ensuite

- Après la configuration de l'agent, vous pouvez démarrer l'instance d'agent en exécutant la commande :

  rép_install/bin/openstack-agent.sh start *nom_instance*

  où *nom_instance* représente le nom de l'instance d'agent à configurer.
- Pour connecter l'Agent OpenStack à un environnement OpenStack activé pour SSL, spécifiez le répertoire du certificat SSL de votre serveur OpenStack en définissant la variable suivante :

  OS_cert_path=*répertoire du fichier certificate.crt*

  La variable OS_cert_path se trouve dans la section OS_authentication_info du fichier ksg_dc_*nom_instance*.cfg.
- Si vous souhaitez collecter des informations sur le processus, configurez le collecteur de données de l'Agent OpenStack en effectuant les étapes de la rubrique «Activation de la collecte des informations liées aux processus et des connexions SSH», à la page 570.
- Si vous souhaitez modifier le niveau de trace de l'agent à des fins d'identification et de résolution des problèmes, éditez la valeur de la variable **KBB_RAS1** dans le fichier *rép_install*/config/sg.environment en suivant les instructions du fichier.

Activation de la collecte des informations liées aux processus et des connexions SSH

Si vous souhaitez collecter des informations sur le processus, configurez le collecteur de données d'agent pour l'Agent OpenStack et configurez les connexions SSH avec le serveur de composant OpenStack cible.

Pourquoi et quand exécuter cette tâche

Vous devez configurer une connexion SSH pour collecter des informations avant de démarrer l'Agent OpenStack. Pour configurer la connexion, utilisez l'outil d'assistance **ksg_setup_key.sh** ou **ksg_ssh_setup.py** fourni par le produit et décrit dans la procédure ci-après.

Si vous êtes habitué aux connexions SSH, vous pouvez également utiliser les commandes Linux **ssh-keygen** et **ssh-copy-id** pour configurer la connexion.

Procédure

1. Accédez au répertoire *rép_install*/config, où *rép_install* est le répertoire d'installation de l'agent.
2. Editez le fichier ksg_dc_*nom_instance*.cfg où *nom_instance* est le nom spécifié pour l'instance d'agent. Le fichier est créé après le démarrage de l'instance d'agent. Si le fichier n'existe pas, copiez *rép_install*/lx8266/sg/bin/ksg_dc.cfg dans le répertoire *rép_install*/config et renommez le fichier ksg_dc_*nom_instance*.cfg. Par exemple, si le nom d'instance est OS1, changez le nom en ksg_dc_OS1.cfg.
3. Dans le fichier ksg_dc_ *nom_instance* .cfg, définissez la valeur du paramètre **collect_process_information** sur YES.
4. Dans la section **OS_process_collection**, spécifiez la valeur du paramètre **ssh_user_host** avec les utilisateurs et les noms d'hôte ou adresses IP des serveurs de composant OpenStack, en respectant le format de l'exemple suivant :

   ```
   ssh_user_host=root@9.112.250.248,user1@hostname
   ```
5. Sauvegardez les paramètres.
6. Pour que les paramètres soient pris en compte, redémarrez l'instance d'agent en exécutant les commandes suivantes :

   ```
   rép_install/bin/openstack-agent.sh stop nom_instance
   rép_install/bin/openstack-agent.sh start nom_instance
   ```
7. Configurez les connexions SSH avec le serveur de composant cible à l'aide d'une des méthodes suivantes :
   - Configurez les connexions une par une à l'aide du script ksg_setup_key.sh : accédez au répertoire *rép_install*/lx8266/sg/bin et exécutez le script ksg_setup_key.sh avec le nom d'hôte ou l'adresse IP et l'utilisateur pour établir les connexions SSH avec les serveurs de composant spécifiés à l'étape 4. Si vous suivez l'exemple de l'étape 4, vous devez exécuter le script deux fois pour configurer les connexions une par une :

     ```
     ./ksg_setup_key.sh 9.112.250.248 root
     ./ksg_setup_key.sh hostname user1
     ```

     Remarque : Vous devez fournir les mots de passe quand vous exécutez les scripts pour la première fois. Vous n'avez pas besoin de fournir de nouveau les mots de passe.
   - Configurez les connexions une par une dans un travail par lots, à l'aide de l'outil ksg_ssh_setup.py fourni par l'Agent OpenStack dans le répertoire *rép_install*/lx8266/sg/bin. Vous devez installer la bibliothèque Python pexpect avant d'utiliser cet outil.
     – Pour configurer les connexions SSH une par une, exécutez la commande :

       ```
       python ksg_ssh_setup.py -single
       ```

       Cette commande vous aide à configurer la connexion SSH au serveur cible distant. Vous devez fournir les informations suivantes :

```
Entrez
le nom d'hôte ou l'adresse IP de la machine cible distante : (entrez
'END' pour terminer l'entrée.)
Entrez le compte pour accéder à la machine distante (par exemple
superutilisateur) :
Entrez le mot de passe de l'utilisateur ci-dessus
:
```

– Pour configurer des connexions de SSH dans un travail par lots, exécutez la commande :

```
python ksg_ssh_setup.py -ssh
fichier_SSH
```

où *fichier_SSH* est le fichier qui contient le serveur cible, l'utilisateur et le mot de passe. Vous devez créer le fichier selon le fichier `ksg_dc_ssh_list.txt` dans le même répertoire que l'outil Python, puis indiquer l'hôte et les informations utilisateur dans le fichier selon le format des exemples :

```
hostname root passw0rd
9.112.250.248 user1 passw0rd
```

Remarque : vous devez les configurer de nouveau seulement en cas de changement de nom d'utilisateur ou de mot de passe pour le serveur cible. Vous n'avez pas besoin de configurer de nouveau les connexions après avoir redémarré l'agent ou changé la configuration de l'agent.

Résultats

Le collecteur de données est configuré et les connexions SSH sont configurées correctement. Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent OpenStack au tableau de bord des performances des applications. Lorsque vous ajoutez l'instance d'agent, sélectionnez **Environnement OpenStack** dans la liste des composants.

Que faire ensuite

- Lorsque vous cliquez sur **API End Point Summary By Sevice Type** > **Détails de noeuds finals d'API**, un message `Aucune donnée disponible` apparaît dans les widgets de groupe **Historique du nombre d'échecs de détection d'API** et **Historique du pourcentage d'échecs de détection d'API**. Cliquez sur un noeud final d'API qui apparaît dans **Détails de noeuds finals d'API** pour afficher les données de surveillance dans les deux widgets de groupe.
- Lorsque vous cliquez sur **Récapitulatif des processus par composant** > **Détails de processus** ou **Statut de la connexion au serveur SSH** > **Détails de processus**, un message `Aucune donnée disponible` apparaît dans les widgets de groupe **Historique d'utilisation de l'UC par les processus** et **Historique d'utilisation de la mémoire par les processus**. Cliquez sur un processus qui apparaît dans **Détails de processus** pour afficher les données de surveillance dans les deux widgets de groupe.

Ajout des valeurs de configuration

Vous devez fournir les valeurs des configurations locale et distante nécessaires au fonctionnement de l'agent.

Si vous utilisez le mode interactif pour configurer l'agent, un panneau est affiché pour que vous puissiez entrer chaque valeur. S'il existe une valeur par défaut, celle-ci figure déjà dans la zone. Si une zone représente un mot de passe, deux zones de saisie s'affichent. Vous devez entrer la même valeur dans chaque zone. Les valeurs que vous entrez ne s'affichent pas de manière à préserver la sécurité de ces valeurs.

Si vous utilisez le mode silencieux pour configurer l'agent, vous pouvez éditer le fichier *fichier_réponses* dans le répertoire *rép_install*`/samples` pour ajouter les valeurs de configuration. Une fois que vous avez sauvegardé les modifications, suivez les instructions de l'étape 6, à la page 569 et exécutez la commande suivante pour que les modifications soient appliquées :

rép_install`/bin/openstack-agent.sh start` *nom_instance*

où *nom_instance* représente le nom de l'instance d'agent à configurer.

Une fois la configuration terminée, vous trouverez les valeurs configurées dans le fichier `.cfg` de l'instance d'agent, par exemple, *`nom_hôte`*`_sg_`*`nom_instance`*`.cfg`.

La configuration de cet agent est organisée en groupes :

Informations d'authentification d'environnement OpenStack (OPENSTACK_CONNECTION)
Informations d'authentification d'environnement OpenStack

Les éléments de configuration définis dans ce groupe figurent toujours dans la configuration de l'agent.

Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

URL d'authentification OpenStack (KSG_OPENSTACK_AUTH_URL)
auth_url de l'environnement OpenStack

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : `http://localhost:identity/v3`

Mot de passe OpenStack (KSG_OPENSTACK_PASSWORD)
Mot de passe de l'administrateur

Type : mot de passe.

Cette valeur est requise.

Valeur par défaut : Néant

Nom du titulaire OpenStack (KSG_OPENSTACK_TENANT_NAME)
Nom du titulaire OpenStack, également connu comme nom de projet

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : admin

Nom d'utilisateur OpenStack (KSG_OPENSTACK_USERNAME)
Administrateur devant se connecter à l'environnement OpenStack

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : admin

Python (KSG_PYTHON)
Emplacement de l'exécutable Python

Les éléments de configuration définis dans ce groupe figurent toujours dans la configuration de l'agent.

Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

Emplacement de l'exécutable Python (KSG_PYTHON_LOCATION)
Exécutable Python qui sera utilisé pour exécuter le collecteur de données de l'agent OpenStack. Vous pouvez rechercher le chemin complet en exécutant la commande suivante dans votre terminal : "which python".

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : Néant

Socket (KSG_SOCKET)
Source de données de socket

Les éléments de configuration définis dans ce groupe sont toujours présents dans la configuration de l'agent.

Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

Numéro de port (CP_PORT)
Port sur lequel l'agent est à l'écoute des données provenant des clients du socket. La valeur 0 indique qu'un port éphémère sera utilisé. Ce port ne correspond à AUCUN port utilisé par votre application. Il est réservé à un usage interne par l'agent.

Type : numérique.

Cette valeur est facultative.

Valeur par défaut : 0

Configuration de la surveillance d'Oracle Database

L'Monitoring Agent for Oracle Database fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de la base de données Oracle. Vous pouvez configurer plusieurs instances d'Agent Oracle Database pour surveiller différentes bases de données Oracle. La fonction de surveillance à distance est également fournie par cet agent.

Avant de commencer

- Avant de configurer Agent Oracle Database, vous devez accorder des privilèges au compte utilisateur Oracle utilisé par Agent Oracle Database. Pour plus d'informations sur les privilèges, voir Accord de privilèges à l'utilisateur de l'agent de base de données Oracle.
- Si vous surveillez une base de données Oracle à distance, l'agent doit être installé sur un ordinateur sur lequel le logiciel de base de données Oracle ou Oracle Instant Client est installé.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent.

Pour la surveillance des performances générales de la base de données Oracle, Agent Oracle Database permet de surveiller la disponibilité, les performances, l'utilisation des ressources et les activités de la base de données Oracle, par exemple :

- Disponibilité des instances dans la base de données Oracle surveillée.
- Informations de ressources, telles que mémoire, caches, segments, limitation, espace table, annulation (rollback), attribut système et statistiques système.
- Informations d'activité, telles que statistiques SE, sessions, conflit et journal des alertes.

L'Agent Oracle Database est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement. De plus, chaque instance d'agent peut surveiller plusieurs bases de données.

Le nom de système géré de l'Agent Oracle Database comprend un nom de connexion de base de données que vous indiquez, un nom d'instance d'agent que vous indiquez et le nom d'hôte de l'ordinateur sur lequel l'agent est installé. Par exemple, `pc:nom_connexion-nom_instance-nom_hôte:SUB`, où *pc* est votre code produit de deux caractères et *SUB* est le type de base de données (les valeurs possibles sont RDB, ASM, ou DG). Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 23 caractères, moins la longueur du nom d'hôte et celle du nom de connexion de base de données. Par exemple, si vous spécifiez **dbconn** comme nom de connexion de base de données, **Oracle02** comme nom d'instance d'agent

et que votre nom d'hôte est *Prod204a*, le système géré s'appelle `RZ:dbconn-oracle02-Prod204a:RDB`. Cet exemple utilise 22 des 23 caractères disponibles pour le nom de connexion de base de données, le nom d'instance d'agent et le nom d'hôte.

- Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.
- La longueur des variables *nom_connexion*, *nom_instance* et *nom_hôte* est tronquée si elle dépasse 23 caractères.
- Pour éviter qu'un nom de sous-noeud soit tronqué, modifiez la convention de dénomination du sous-noeud en paramétrant les variables d'environnement suivantes : **KRZ_SUBNODE_INCLUDING_AGENTNAME**, **KRZ_SUBNODE_INCLUDING_HOSTNAME** et **KRZ_MAX_SUBNODE_ID_LENGTH**.
- Si vous attribuez la valeur `NO` à la variable **KRZ_SUBNODE_INCLUDING_AGENTNAME**, la partie ID sous-noeud du nom de sous-noeud ne contient pas le nom de l'instance d'agent. Par exemple,
  - Nom de sous-noeud par défaut : *ConnexionBD-Instance-nomHôte*
  - Nom de sous-noeud avec variable d'environnement définie sur `NO` : *ConnexionBD-nomHôte*
- Si vous définissez **KRZ_SUBNODE_INCLUDING_HOSTNAME** sur `NO`, la partie ID sous-noeud du nom de sous-noeud ne contient pas le nom d'hôte. Par exemple,
  - Nom de sous-noeud par défaut : *ConnexionBD-Instance-nomHôte*
  - Nom de sous-noeud avec variable d'environnement définie sur `NO` : *ConnexionBD-Instance*

Procédure

1. Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 575.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 582.
2. Pour configurer l'agent sur des systèmes d'exploitation Linux et UNIX, vous pouvez exécuter le script et répondre aux invites ou utiliser le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 578.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 582.

Que faire ensuite

Pour la configuration avancée uniquement, l'administrateur de la base de données Oracle doit permettre à l'utilisateur Oracle d'exécuter le script `krzgrant.sql` pour accéder à la base de donnés. Voir Exécution du script krzgrant.sql.

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management. Une fois que vous avez mis à jour les valeurs de configuration, démarrez l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Agent de surveillance pour Oracle Database**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Dans la fenêtre Monitoring Agent for Oracle Database, procédez comme suit :
   a. Entrez un nom d'instance unique pour l'instance d'Monitoring Agent for Oracle Database et cliquez sur **OK**.
4. Dans le panneau Default Database Configuration de la fenêtre Configure ITCAM Extended Agent for Oracle Database, procédez comme suit :
   a. Entrez le **nom d'utilisateur par défaut**. Il s'agit de l'ID utilisateur de la base de données par défaut utilisé pour les connexions à la base de données. Il s'agit de l'ID utilisé par l'agent pour accéder à l'instance de la base de données surveillée. Cet ID utilisateur doit disposer de privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.
   b. Entrez le **mot de passe par défaut**. Il s'agit du mot de passe associé à l'ID utilisateur de la base de données par défaut spécifié.
   c. Si la version de l'agent Oracle est 8.0, procédez comme suit.
      1) Entrez le **fichier jar d'Oracle JDBC**. Il s'agit du chemin complet du fichier jar du pilote Oracle JDBC utilisé pour communiquer avec la base de données Oracle. Le pilote Oracle Java Database Connectivity (JDBC) qui prend en charge les versions de la base de données Oracle surveillées par l'agent Oracle doit être disponible sur l'ordinateur de l'agent.
   d. Si la version de l'agent Oracle est 6.3.1.10, procédez comme suit.
      1) Si l'Agent Oracle Database est installé sur le serveur de base de données Oracle surveillé, sélectionnez **Use libraries in Oracle home** et entrez le **répertoire de base d'Oracle**. (Facultatif) Le paramètre `Oracle Home Directory` peut ne pas être défini pour la surveillance locale ; la variable d'environnement système *ORACLE_HOME* sera utilisée.
      2) Si l'Agent Oracle Database est distant du serveur de base de données Oracle surveillé, sélectionnez **Use libraries in Oracle instant client** et entrez le **répertoire d'installation du client Oracle Instant**.
   e. Pour définir les options de configuration avancées, cochez **Show advanced options** ; sinon, passez à l'étape 5.
   f. Le paramètre `Net Configuration Files Directories` peut ne pas être défini et le répertoire par défaut est utilisé. Si la version de l'agent Oracle est 6.3.1.10, vous pouvez indiquer plusieurs répertoires de fichiers de configuration en séparant leur nom par un point-virgule (;). Pour l'agent Oracle version 8.0, seul un répertoire est pris en charge. Ce paramètre contient le(s) fichier(s) de configuration réseau de la base de données Oracle. Le répertoire est défini par la variable d'environnement *TNS_ADMIN* pour chaque instance de base de données Oracle. Le répertoire par défaut est `%ORACLE_HOME%\NETWORK\ADMIN`. Si cet élément n'est pas configuré, le répertoire par défaut est utilisé. Pour désactiver l'utilisation du répertoire par défaut, définissez la variable d'environnement d'agent suivante sur false : `KRZ_LOAD_ORACLE_NET=false`.
   g. Ne définissez pas le paramètre `Customized SQL definition file name`. Il n'est pas utilisé.

h. Indiquez si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail. Le programme d'écoute dynamique par défaut est `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail, définissez cette valeur sur Yes.

i. Cliquez sur **Suivant**.

5. Dans le panneau **Instance configuration** de la fenêtre Configure ITCAM Extended Agent for Oracle Database, procédez comme suit : Définissez dans ce panneau les instances de connexion à la base de données réelles. Vous devez en ajouter au moins une. Vous pouvez également y éditer et y supprimer des instances de connexion à la base de données. S'il existe plusieurs configurations d'instance de connexion à la base de données, utilisez l'option **Database connections** pour choisir l'instance à éditer ou supprimer.

   a. Appuyez sur **New** dans la section **`Database connections`**.

   b. Définissez un alias pour la connexion à la base de données dans **`Database Connection Name`**. Cet alias vous permet de représenter la connexion à la base de données avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.

   c. Définissez le paramètre **`Connection Type`**

      1) (Facultatif) Basic

         Le type de connexion le plus courant et par défaut est **Basic**. Si vous n'êtes pas sûr du type de connexion dont vous avez besoin, il est recommandé de choisir celui-ci.

         a) Sélectionnez le type de connexion **Basic** lorsque la base de données cible surveillée est une instance unique, telle qu'une instance de système de fichiers standard ou une instance ASM unique.

         b) Définissez le nom d'hôte ou l'adresse IP de la base de données dans la zone `Hostname`.

         c) Entrez le numéro de port utilisé par la base de données dans la zone `Port`.

         d) Sélectionnez **Service Name** ou **SID**.

            i. Si **Service Name** est sélectionné, entrez le nom du service qui est une représentation logique d'une base de données, une chaîne qui est le nom de service de base de données globale.

               Un nom de service est une représentation logique d'une base de données, à savoir la manière dont une base de données est présentée aux clients. Une base de données peut être présentée sous forme de services multiples et un service peut être implémenté en tant qu'instances de base de données multiples. Le nom de service est une chaîne qui correspond au nom de base de données global, à savoir un nom composé du nom de la base de données et du nom de domaine, saisie lors de l'installation ou de la création de la base de données. Si vous n'êtes pas sûr de connaître le nom de la base de données global, vous pouvez l'obtenir à partir de la valeur du paramètre SERVICE_NAMES dans le fichier de paramètres d'initialisation.

            ii. Si **SID** est sélectionné, entrez l'ID système Oracle qui identifie une instance d'une base de données active.

               Il s'agit de l'identificateur système Oracle qui identifie une instance spécifique d'une base de données.

               Passez à l'étape 5d.

      2) (Facultatif) TNS

         a) Sélectionnez le type de connexion **TNS** si la variable d'environnement système *ORACLE_HOME* est définie et que l'alias TNS de la base de données cible surveillée est défini dans le fichier `$ORACLE_HOME/network/admin/tnsnames.ora`.

         b) Entrez le nom de l'**`alias TNS`**.

            Passez à l'étape 5d.

      3) (Facultatif) Advanced

a) Sélectionnez le type de connexion **avancé** lorsqu'il existe plusieurs instances Oracle dans plusieurs noeuds physiques pour la base de données surveillée. Par exemple, un ASM avec une base de données Real Applications Cluster (RAC).

b) Entrez la **chaîne de connexion Oracle**.

Cet attribut prend en charge toutes les méthodes d'affectation de nom Oracle Net comme suit :

- Chaîne URL SQL Connect de format `://host:port/service name`. Par exemple, `//dlsun242:1521/bjava21`.
- Paire mot clé-valeur Oracle Net. Par exemple,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entrées **TNSNAMES**, telles que **inst1** avec la variable d'environnement *TNS_ADMIN* ou *ORACLE_HOME* définie et les fichiers de configuration configurés.

Passez à l'étape 5d.

d. Cochez **Use a different user name and password** pour que cette connexion utilise des données d'identification différentes de celles par défaut que vous avez définies à l'étape 4a et à l'étape 4b ci-dessus. Sinon, passez à l'étape 5g.

e. Entrez le **nom d'utilisateur de la base de données** pour cette connexion. Il s'agit de l'ID utilisé par l'agent pour accéder à l'instance de la base de données surveillée. Cet ID utilisateur doit disposer de privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.

f. Entrez le **mot de passe de la base de données**. Il s'agit du mot de passe associé à l'ID utilisateur de base de données spécifié.

g. Sélectionnez un **rôle** qui correspond aux droits accordés aux données d'identification de la connexion à la base de données. Le rôle est l'ensemble de privilèges à associer à la connexion. Pour un utilisateur disposant du privilège système SYSDBA, indiquez un rôle qui comprend ce privilège. Pour les instances ASM, utilisez le rôle **SYSDBA** ou **SYSASM**.

h. Cochez **Show remote log monitoring options** si vous surveillez des journaux d'alertes Oracle distants à partir de cette instance d'agent ; sinon, passez à l'étape 5k.

i. Entrez le **chemin d'accès au fichier journal des alertes Oracle** ou utilisez **Browse** pour le sélectionner. Chemins d'accès complets des fichiers journaux d'alertes mappés des instances distantes de cette connexion de la base de données. L'agent surveille les journaux d'alertes en lisant ces fichiers. Ils se trouvent généralement à l'emplacement `$ORACLE_BASE/diag/rdbms/`*`NOM_BDD`*`/`*`ID_SYS`*`/trace/alert_`*`ID_SYS`*`.log`. Par exemple, si *NOM_BDD* et *ID_SYS* sont définis sur `db11g` et *ORACLE_BASE* est défini sur `/home/dbowner/app/oracle`, le journal des alertes figure à l'emplacement `/home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log`.

Windows Si l'Agent Oracle Database s'exécute et lit les fichiers journaux d'alerte via le réseau, le chemin de fichier distant doit suivre la convention de dénomination universelle des systèmes Windows. Par exemple, `\\tivx015\path\alert_orcl.log`.

Windows

Important : Entrez à la fois le chemin d'accès et le nom du fichier journal des alertes. Aucun pilote de réseau mappé n'est pris en charge pour les chemins des journaux d'alertes.

Linux AIX Si l'Agent Oracle Database se trouve sur un serveur distant, un système de fichiers monté en local est requis pour surveiller ses journaux d'alertes distants.

Windows Séparez plusieurs fichiers par un point-virgule (;).

Linux AIX Plusieurs fichiers sont séparés par un signe deux-points (:).

Chaque fichier est mis en correspondance avec une instance de base de données en utilisant le modèle de nom de fichier `alert_`*`instance`*`.log`. S'il n'existe pas de correspondance, il est ignoré.

Les fichiers journaux des alertes de l'instance locale de la base de données sont reconnus automatiquement.

j. Sélectionnez ou saisissez le **jeu de caractères du fichier journal des alertes Oracle**. Il s'agit de la page de codes des fichiers journaux des alertes mappés. Si ce paramètre est vide, les paramètres régionaux en cours du système sont utilisés, par exemple :
   - ISO8859_1, ISO 8859-1 Europe occidentale
   - UTF-8, UTF-8 Unicode
   - GB18030, chinois simplifié GB18030
   - CP950, chinois traditionnel
   - EUC_JP, japonais
   - EUC_KR, coréen

   Pour la liste complète des pages de codes, voir Pages de codes prises en charger ICU.

k. Cliquez sur **Apply** pour sauvegarder les paramètres de cette instance de connexion à la base de données dans la section **Database connections**.

l. (Facultatif) Testez la connexion à la nouvelle base de données.
   1) Sélectionnez la nouvelle connexion à la base de données dans la section **Database connections**.
   2) Cliquez sur **Tester la connexion**.
   3) Observez les résultats dans la fenêtre Tester la connexion.
      - Exemple de **résultat au test** réussi :

        ```
        Testing connection config1 ...
        Success
        ```

      - Exemple de **résultat au test** échoué :

        ```
        Testing connection config1 ...
        KBB_RAS1_LOG; Set MAXFILES to 1
        ORA-12514: TNS:listener does not currently know of service requested in connect descriptor
        Failed
        ```

m. Cliquez sur **Suivant**.

6. Lisez les informations contenues dans le panneau **Summary** de la fenêtre Configure ITCAM Extended Agent for Oracle Database, puis cliquez sur **OK** pour terminer la configuration d'une instance d'agent.
7. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour Oracle Database**, puis cliquez sur **Start**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent en répondant à des invites

Pour configurer l'agent sur des systèmes d'exploitation Linux et UNIX, exécutez le script de configuration de ligne de commande et répondez à ses invites.

Procédure

1. Ouvrez le répertoire *rép_install*/bin, où *rép_install* est le répertoire d'installation de l'Agent Oracle Database.
2. (Facultatif) Pour répertorier les noms des éventuelles instances d'agent configurées existantes, exécutez la commande **./cinfo -o rz**.
3. Pour configurer l'Agent Oracle Database, exécutez la commande **./oracle_database-agent.sh config** *nom_instance*.
4. A l'invite Edit 'Monitoring Agent for Oracle Database' settings, appuyez sur **Entrée**. La valeur par défaut est Oui.
5. Pour entrer les informations sur la configuration de base de données par défaut, procédez comme suit :

Remarque : La section `Configuration par défaut de base de données` ne correspond pas à la configuration de l'instance de connexion à la base de données. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut lorsque vous ajoutez les configurations d'instance de connexion à la base de données réelles, qui commence à l'étape 6.

a. Lorsque le système demande de saisir le `nom d'utilisateur par défaut`, entrez l'ID utilisateur de la base de données par défaut pour les connexions à la base de données et appuyez sur **Entrée**. Il s'agit de l'ID utilisé par l'agent pour accéder à l'instance de la base de données surveillée. Cet ID utilisateur doit disposer de privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.

b. Lorsque le système demande de saisir le `mot de passe par défaut`, tapez le mot de passe associé à l'ID utilisateur de base de données par défaut défini et appuyez sur **Entrée**. Confirmez ensuite le mot de passe si le système vous le demande.

c. Si la version de l'agent Oracle est 8.0, procédez comme suit.

   1) Entrez le **`fichier jar d'Oracle JDBC`**. Il s'agit du chemin complet du fichier jar du pilote Oracle JDBC utilisé pour communiquer avec la base de données Oracle. Le pilote Oracle Java Database Connectivity (JDBC) qui prend en charge les versions de la base de données Oracle surveillées par l'agent Oracle doit être disponible sur l'ordinateur de l'agent.

d. Si la version de l'agent Oracle est 6.3.1.10, procédez comme suit.

   1) Lorsque le système demande de saisir le `répertoire de base Oracle`, si l'Agent Oracle Database est installé sur le serveur de base de données Oracle surveillé, entrez le `répertoire de base Oracle` et appuyez sur **Entrée**. Si l'Agent Oracle Database n'est pas installé sur le serveur de base de données Oracle qui va être surveillé, ne définissez pas ce paramètre, appuyez sur **Entrée** et passez à l'étape suivante. Pour effacer la valeur du `répertoire de base Oracle`, appuyez sur la barre d'espace, puis sur **Entrée**.

      Remarque : (Facultatif) Vous pouvez ne pas définir le `répertoire de base Oracle` et le `répertoire d'installation du client Oracle Instant` pour la surveillance locale ; la variable d'environnement système *ORACLE_HOME* sera utilisée.

   2) Si l'Agent Oracle Database est éloigné du serveur de base de données Oracle surveillé, entrez le `répertoire d'installation du client Oracle Instant` et appuyez sur **Entrée**. Si vous avez défini le `répertoire de base Oracle` à l'étape 5d1, cette valeur est ignorée.

e. Le paramètre `Net Configuration Files Directories` peut ne pas être défini et le répertoire par défaut est utilisé. Si la version de l'agent Oracle est 6.3.1.10, vous pouvez saisir plusieurs répertoires de fichiers de configuration en utilisant Windows ";" ou Linux AIX ":" pour séparer les répertoires. Pour l'agent Oracle version 8.0, seul un répertoire est pris en charge. Appuyez sur **Entrée**. Ce paramètre contient le(s) fichier(s) de configuration réseau de la base de données Oracle. Le répertoire est défini par la variable d'environnement *TNS_ADMIN* pour chaque instance de base de données Oracle. Le répertoire par défaut est Linux AIX `$ORACLE_HOME/network/admin` ou Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Si cet élément n'est pas configuré, le répertoire par défaut est utilisé. Pour désactiver l'utilisation du répertoire par défaut, définissez la variable d'environnement d'agent suivante sur false : `KRZ_LOAD_ORACLE_NET=false`.

f. Indiquez si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail, puis appuyez sur **Entrée**. Le programme d'écoute dynamique par défaut est `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail, définissez cette valeur sur True.

g. Ne définissez pas le paramètre `Customized SQL definition file name`. Il n'est pas utilisé.

6. L'invite `Edit 'Database Connection' settings` apparaît une fois que la sortie suivante s'affiche à l'écran :

```
Instance Configuration :
Summary :
Database Connection :
```

Remarque : Définissez dans cette étape les instances de connexion à la base de données réelles. Vous devez en ajouter au moins une. Vous pouvez également y éditer et y supprimer des instances de connexion à la base de données. S'il existe plusieurs configurations d'instance de connexion à la base de données, utilisez l'option `Next` pour ignorer les instances qui n'ont pas besoin d'être modifiées ou supprimées jusqu'à accéder à l'instance que vous devez modifier ou supprimer.

7. Pour ajouter une nouvelle connexion de base de données, tapez 1 et appuyez sur **Entrée**.
8. Pour entrer les informations de connexion de base de données par défaut, procédez comme suit :
   a. Lorsque le système demande le `nom de connexion à la base de données`, tapez un alias pour la connexion à la base de données, puis appuyez sur **Entrée**. Cet alias vous permet de représenter la connexion à la base de données avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.
   b. Lorsque le système demande le `type de connexion`, sélectionnez l'un des types de connexion suivants :
      1) (Facultatif) Basic

         Le type de connexion le plus courant et par défaut est **Basic**. Si vous n'êtes pas sûr du type de connexion dont vous avez besoin, il est recommandé de choisir celui-ci.

         a) Sélectionnez le type de connexion **Basic** si la base de données cible surveillée est une instance unique, telle qu'une instance de système de fichiers standard ou une instance ASM unique.
         b) Lorsque le système demande le `nom d'hôte`, tapez le nom d'hôte ou l'adresse IP de la base de données Oracle et appuyez sur **Entrée**.
         c) Lorsque le système demande le `port`, tapez le numéro de port et appuyez sur **Entrée**.
         d) Entrez l'un des deux paramètres suivants : `Service Name` ou `SID`.
            i. (Facultatif) Lorsque le système demande le `nom du service`, tapez le nom du service qui est une représentation logique d'une base de données, une chaîne qui est le nom de service de base de données globale, appuyez sur **Entrée** et passez à l'étape 8c.

               Un nom de service est une représentation logique d'une base de données, à savoir la manière dont une base de données est présentée aux clients. Une base de données peut être présentée sous forme de services multiples et un service peut être implémenté en tant qu'instances de base de données multiples. Le nom de service est une chaîne qui correspond au nom de base de données global, à savoir un nom composé du nom de la base de données et du nom de domaine, saisie lors de l'installation ou de la création de la base de données. Si vous n'êtes pas sûr de connaître le nom de la base de données global, vous pouvez l'obtenir à partir de la valeur du paramètre SERVICE_NAMES dans le fichier de paramètres d'initialisation. Ce paramètre peut rester vide si vous définissez `SID` à l'étape 8b1dii.

            ii. (Facultatif) Lorsque le système demande le `SID`, tapez le SID (System Identifier) Oracle qui identifie une instance d'une base de données active, appuyez sur **Entrée** et passez à l'étape 8c.

               Ce paramètre est l'identificateur système Oracle qui identifie une instance spécifique d'une base de données. Si le `nom de service` a été défini à l'étape 8b1di, vous pouvez ne pas définir cet élément.

      2) (Facultatif) TNS
         a) Sélectionnez le type de connexion **TNS** lorsque la variable d'environnement système *ORACLE_HOME* est définie et que l'alias TNS de la base de données cible surveillée est défini dans le fichier `$ORACLE_HOME/network/admin/tnsnames.ora`.
         b) Tapez le nom d'alias TNS, appuyez sur **Entrée** et passez à l'étape 8c.
      3) (Facultatif) Advanced

a) Sélectionnez le type de connexion **avancé** lorsqu'il existe plusieurs instances Oracle dans plusieurs noeuds physiques pour la base de données surveillée. Par exemple, un ASM avec une base de données Real Applications Cluster (RAC).

b) Tapez la chaîne de connexion Oracle, appuyez sur **Entrée** et passez à l'étape 8c.

Cet attribut prend en charge toutes les méthodes d'affectation de nom Oracle Net comme suit :

- Chaîne URL SQL Connect de format `://host:port/service name`. Par exemple, `//dlsun242:1521/bjava21`.
- Paire mot clé-valeur Oracle Net. Par exemple,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entrées **TNSNAMES**, telles que **inst1** avec la variable d'environnement *TNS_ADMIN* ou *ORACLE_HOME* définie et les fichiers de configuration configurés.

Remarque : La description qui s'affiche lors de la configuration de ligne de commande peut contenir une barre oblique inversée avant le signe deux points (\:) et le signe égal (\=). Ne saisissez pas de barre oblique inversée dans la chaîne de connexion. Cette barre s'affiche dans la description pour mettre en échappement le comportement normal d'interprétation du signe égal dans une commande et l'interpréter sous la forme de texte.

c) Passez à l'étape 8c.

c. Lorsque le système demande le `nom d'utilisateur de base de données`, tapez l'ID utilisateur de base de données de la connexion et appuyez sur **Entrée**.

Pour les instances de système de fichiers standard, cet ID utilisateur doit disposer des privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.

Pour les instances ASM, utilisez un compte disposant du rôle **SYSDBA** ou **SYSASM**. Par exemple, le compte sys.

d. Lorsque le système demande le `mot de passe de base de données`, tapez le mot de passe associé à l'ID utilisateur de base de données défini.

e. Lorsque le système demande le `rôle`, sélectionnez le rôle qui correspond aux droits accordés à l'ID utilisateur spécifié et appuyez sur **Entrée**.

Le rôle est l'ensemble de privilèges à associer à la connexion. Pour un utilisateur disposant du privilège système SYSDBA, indiquez un rôle qui comprend ce privilège.

Pour les instances ASM, utilisez le rôle **SYSDBA** ou **SYSASM**.

f. Lorsque le système demande les `chemins des fichiers journaux d'alertes Oracle (y compris le nom du fichier journal des alertes)`, tapez les chemins des journaux d'alerte et appuyez sur **Entrée**.

Ce paramètre concerne les chemins d'accès complets des fichiers journaux d'alertes mappés des instances distantes de cette connexion de la base de données. L'agent surveille les journaux d'alertes en lisant ces fichiers. Ils se trouvent généralement à l'emplacement `$ORACLE_BASE/diag/rdbms/`*`NOM_BDD`*`/`*`ID_SYS`*`/trace/alert_`*`ID_SYS`*`.log`. Par exemple, si *NOM_BDD* et *ID_SYS* sont définis sur `db11g` et *ORACLE_BASE* est défini sur `/home/dbowner/app/oracle`, le journal des alertes figure à l'emplacement `/home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log`.

Windows Si l'Agent Oracle Database s'exécute et lit les fichiers journaux d'alerte sur le réseau, le chemin de fichier distant doit suivre la convention de dénomination universelle des systèmes Windows. Par exemple, `\\tivx015\path\alert_orcl.log`.

Important : Entrez à la fois le chemin d'accès et le nom du fichier journal des alertes. Aucun pilote de réseau mappé n'est pris en charge pour les chemins des journaux d'alertes.

Linux AIX Si l'Agent Oracle Database s'exécute, un système de fichiers monté localement est requis pour les journaux d'alertes distants.

Windows Séparez plusieurs fichiers par un point-virgule (;).

Linux AIX Plusieurs fichiers sont séparés par un signe deux-points (:).

Chaque fichier est mis en correspondance avec une instance de base de données en utilisant le modèle de nom de fichier `alert_instance.log`. S'il n'existe pas de correspondance, il est ignoré.

Les fichiers journaux des alertes de l'instance locale de la base de données peuvent être reconnus automatiquement.

g. Lorsque le système demande le **jeu de caractères du fichier journal des alertes Oracle**, tapez la page de codes des fichiers journaux d'alertes associés, puis appuyez sur **Entrée**.

Si ce paramètre est vide, les paramètres régionaux en cours du système sont utilisés, par exemple :

- ISO8859_1, ISO 8859-1 Europe occidentale
- UTF-8, UTF-8 Unicode
- GB18030, chinois simplifié GB18030
- CP950, chinois traditionnel
- EUC_JP, japonais
- EUC_KR, coréen

Pour la liste complète des pages de codes, voir Pages de codes prises en charger ICU.

9. A l'invite `Edit 'Database Connection' settings`, le nom de la connexion à la base de données que vous avez défini à l'étape 8a s'affiche. Vous pouvez l'éditer à nouveau ou le supprimer. Si plusieurs instances de connexion à la base de données sont déjà configurées, cliquez sur **Next** pour les parcourir.
10. (Facultatif) Pour ajouter une autre connexion à la base de données afin de surveiller plusieurs instances de base de données avec cette instance d'agent, entrez 1, appuyez sur **Entrée** et revenez à l'étape 8.
11. Une fois que vous avez terminé de modifier les connexions à la base de données, entrez 5 et appuyez sur **Entrée** pour quitter le processus de configuration.
12. Pour démarrer l'agent, entrez la commande suivante : *rép_install*`/bin/oracle_database-agent.sh start` *nom_instance*.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Ouvrez le fichier `oracle_silent_config.txt` dans un éditeur de texte :
   - Linux AIX *rép_install*`/samples/oracle_database_silent_config.txt`.
   - Windows *rép_install*`\samples\oracle_database_silent_config.txt`
2. Pour **`Default Username`**, entrez le nom de l'utilisateur de base de données par défaut pour les connexions à la base de données qui sont créées pour cette instance d'agent. Par exemple, **`KRZ_CONN_USERID=`**`user1`.

   Remarque : Cet utilisateur doit disposer de privilèges suffisants pour exécuter les tâches, telles que l'interrogation des tables, que cet agent exécute lorsqu'il est connecté à la base de données.
3. Pour **`Default Password`**, vous devez entrer le mot de passe associé à l'utilisateur de base de données par défaut spécifié. Par exemple, **`KRZ_CONN_PASSWORD=`**`mot de passe`.
4. Si la version de l'agent Oracle est 8.0, procédez comme suit.
   a. Entrez le **`fichier jar d'Oracle JDBC`**. Il s'agit du chemin complet du fichier jar du pilote Oracle JDBC utilisé pour communiquer avec la base de données Oracle. Le pilote Oracle Java Database Connectivity (JDBC) qui prend en charge les versions de la base de données Oracle surveillées par l'agent Oracle doit être disponible sur l'ordinateur de l'agent.
5. Si la version de l'agent Oracle est 6.3.1.10, procédez comme suit.
   a. Si l'Agent Oracle Database est installé sur le serveur de base de données Oracle surveillé, entrez le `répertoire de base Oracle`. Par exemple, **`KRZ_ORACLE_HOME=`**`chemin du répertoire de base`.

      Remarque : pour les paramètres facultatifs comme celui-ci, supprimez le symbole dièse (#) en préfixe pour les utiliser.
      Si l'Agent Oracle Database n'est pas installé sur le serveur de base de données Oracle qui va être surveillé, ne définissez pas ce paramètre et passez à l'étape suivante.

      Remarque : (facultatif) vous pouvez ne pas définir le `répertoire de base Oracle` et le `répertoire d'installation du client Oracle Instant` (mise en commentaire en insérant le symbole dièse (#) à la première position de la ligne du paramètre dans le fichier texte de configuration en mode silencieux) ; la variable d'environnement système *ORACLE_HOME* sera utilisée.
   b. Si l'Agent Oracle Database est éloigné du serveur de base de données Oracle surveillé, entrez le `répertoire d'installation du client Oracle Instant`. Si vous avez saisi le `répertoire de base Oracle` à l'étape précédente, cette valeur est ignorée.
      - Windows Définissez le chemin de dossier complet du répertoire de **`base Oracle`** qui contient les fichiers de la bibliothèque `Oracle Call Interface (OCI)`. Si le chemin complet du fichier `oci.dll` est `C:\instantclient_10_2\oci.dll`, vous devez définir le chemin `C:\instantclient_10_2`. Par exemple, **`KRZ_INSTANT_CLIENT_LIBPATH=`**`C:\instantclient_10_2`
      - AIX Définissez le chemin de dossier complet du répertoire de **`base Oracle`** qui contient les fichiers de la bibliothèque `Oracle Call Interface (OCI)`. Si le chemin complet du fichier `libocci.so.10.1` est `/home/tivoli/oci/libocci.so.10.1`, vous devez définir le chemin `/home/tivoli/oci`. Par exemple, **`KRZ_INSTANT_CLIENT_LIBPATH=`**`/home/tivoli/oci`
6. Le paramètre `Net Configuration Files Directories` peut ne pas être défini et le répertoire par défaut est utilisé. Agent Oracle Database utilise ce chemin de fichier pour obtenir le fichier `tnsnames.ora`. Ce répertoire est défini par la variable d'environnement *TNS_ADMIN* pour chaque instance de base de données Oracle. Le répertoire par défaut est Linux AIX `$ORACLE_HOME/network/admin` ou Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Si vous définissez ce paramètre avec plusieurs répertoires de fichiers de configuration réseau, utilisez Windows ";" ou Linux AIX ":" pour séparer les répertoires.
   Si vous surveillez des bases de données Oracle à distance, vous pouvez copier les fichiers de configuration réseau du système distant vers le système où l'agent est installé. En outre, vous

pouvez fusionner le contenu des fichiers de configuration réseau sur le système distant avec les fichiers de configuration réseau sur le système où l'agent est installé.

7. Pour l'**écoute dynamique**, vérifiez que le programme d'écoute dynamique est configuré. Le programme d'écoute dynamique par défaut est (PROTOCOL=TCP)(HOST=localhost)(PORT=1521). Si le programme d'écoute dynamique par défaut est configuré, définissez cette valeur sur TRUE comme indiqué ici ; **KRZ_DYNAMIC_LISTENER=**TRUE.

   Les valeurs valides sont TRUE et FALSE.

8. Ne définissez pas le paramètre `Customized SQL definition file name`. Il n'est pas utilisé.
9. Les instances de connexion à la base de données réelles sont définies à partir de cette étape. Vous devez en ajouter au moins une. Les entrées d'une instance sont fournies dans le fichier `oracle_silent_config.txt` avec le nom d'instance *config1*. Si vous modifiez le nom d'instance, veillez à modifier toutes les références.

   Cet alias vous permet de représenter la connexion à la base de données avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.

10. Pour le **type de connexion**, définissez l'un des types de connexion suivants : **De base**, **TNS**, ou **Avancé**. Par exemple, **KRZ_CONN_TYPE.config1=**Basic.
11. Pour le type de connexion que vous avez sélectionné à l'étape précédente, spécifiez les paramètres requis :

    De base

    - Pour le **nom d'hôte**, définissez le nom d'hôte ou l'adresse IP de la base de données Oracle, par exemple, **KRZ_CONN_HOST.config1=** nom_hôte.
    - Pour le **port**, définissez le port d'écoute de la base de données Oracle, par exemple, **#KRZ_CONN_PORT.config1=** 1521.
    - Pour le **nom de service**, définissez la représentation logique de la base de données en utilisant une chaîne pour le nom de base de données global, par exemple, **KRZ_CONN_SERVICE.config1=** orcl.

      Important : Si vous ne définissez pas le nom de service, vous devez spécifier l'identificateur système Oracle (SID).

      Pour le **SID (System Identifier) Oracle**, définissez un SID qui identifie une instance d'une base de données active, par exemple, **KRZ_CONN_SID.config1=** sid.

    TNS Pour l'**alias TNS**, définissez le nom d'alias réseau depuis le fichier `tnsnames.ora`. Par exemple, **KRZ_CONN_TNS.config1=** alias_tns.

    Avancé

    Pour la **chaîne de connexion Oracle**, définissez la chaîne de connexion de base de donnée d'OCI. Par exemple, **KRZ_CONN_STR.config1=** //host:port/service

    Cette chaîne prend en charge toutes les méthodes de dénomination Oracle Net, comme indiqué ci-dessous :

    - Pour une chaîne URL SQL Connect :

      ```
      //host:[port][/service name]
      ```

    - Pour une paire mot clé/valeur Oracle Net

      ```
      "(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=bjava21)))"
      ```

    Cette chaîne prend également en charge les entrées **TNSNAMES** , par exemple, **inst1**, où la variable d'environnement *TNS_ADMIN* ou *ORACLE_HOME* est définie et les fichiers de configuration sont configurés.

    Important : Cet attribut s'applique uniquement au type de connexion avancée.

12. Pour le **nom d'utilisateur de base de données**, vous pouvez définir le nom de l'utilisateur de base de données de la connexion, par exemple, **KRZ_CONN_USERID=**UserID.

    Cet utilisateur doit disposer des privilèges suffisants pour pouvoir exécuter les tâches que l'agent doit exécuter (création, modification et suppression de tables, par exemple) lorsqu'il est connecté à la base de données.

    Si cette zone est vide, l'agent utilise le nom d'utilisateur par défaut dans la section de configuration de base de données par défaut. Si le **nom d'utilisateur de base de données** n'a pas été configuré, le nom d'utilisateur par défaut est utilisé pour la connexion.

13. Pour le **mot de passe de base de données**, vous pouvez définir le mot de passe associé à l'utilisateur de base de données défini, par exemple, **KRZ_CONN_PASSWORD=**Password.

    Si cette zone est vide, l'agent utilise le mot de passe par défaut dans la section de configuration de base de données par défaut. Si le **mot de passe de base de données** n'est pas défini, le mot de passe par défaut est utilisé pour la connexion.

14. Pour le **rôle**, vous pouvez définir l'ensemble de privilèges associés à la connexion, par exemple **KRZ_CONN_MODE.config1=**DEFAULT.

    Les valeurs valides sont notamment *SYSDBA*, *SYSOPER*, *SYSASM* et *DEFAULT*.

    Pour un utilisateur disposant du privilège système *SYSDBA*, vous pouvez définir une connexion qui inclut ce privilège. Si cet élément n'est pas défini, vous pouvez affecter le rôle *DEFAULT* à l'utilisateur.

15. Pour les **chemins des fichiers journaux d'alertes Oracle**, qui incluent le nom de fichier journal des alertes, vous pouvez définir le chemin de fichier absolu des fichiers journaux d'alertes mappés des instances de base de données distante dans cette connexion de base de données. Par exemple, **KRZ_LOG_PATHS.config1=**chemin_journal_alertes.

    Windows Utilisez le point-virgule (;) pour séparer plusieurs fichiers.

    Linux AIX Utilisez le signe deux-points (:) pour séparer plusieurs fichiers.

    Chaque fichier est mis en correspondance avec une instance de base de données par le modèle de nom de fichier alert_*instance*.log. Sinon, il est ignoré si aucune correspondance n'existe.

    Les fichiers journaux d'alertes d'instance de base de données locale sont reconnus automatiquement.

    Si les **chemins des fichiers journaux d'alertes Oracle** n'ont pas été définis, le journal d'alertes n'est pas disponible.

16. Pour le **jeu de caractères des fichiers journaux d'alertes Oracle**, vous pouvez définir la page de codes des fichiers journaux d'alertes associés. Par exemple, **KRZ_LOG_CHARSET.config1=** jeu_caractères

    Si cette zone est vide, les paramètres régionaux en cours du système sont utilisés, comme indiqué ici :

    ```
    ISO8859_1: ISO 8859-1 Western European encoding
    UTF-8: UTF-8 encoding of Unicode
    GB18030: Simplified Chinese GB18030 encoding
    CP950: Traditional Chinese encoding
    EUC_JP: Japanese encoding
    ```

17. Sauvegardez et fermez le fichier oracle_database_silent_config.txt. Entrez :
    rép_install/bin/oracle_database-agent.sh config *nom_instance rép_install*/samples/oracle_database_silent_config.txt
    où *nom_instance* est le nom à attribuer à l'instance.

18. Pour démarrer l'agent, entrez la commande suivante :
    rép_install/bin/oracle_database-agent.sh start *nom_instance*.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Accord de privilèges à l'utilisateur de l'agent de base de données Oracle

Une fois que vous avez installé l'agent, vous devez accorder des privilèges au compte utilisateur Oracle utilisé par Agent Oracle Database.

Vous pouvez accorder des privilèges aux utilisateurs suivants :

- Utilisateurs d'instance (non ASM) de système de fichiers standard
- Utilisateurs non SYS d'instance ASM with RAC

Attribution de privilèges aux utilisateurs pour les instances de système de fichiers standard

Pour les instances de système de fichiers standard, l'ID utilisateur Oracle utilisé par l'Agent Oracle Database doit disposer des privilèges de sélection sur les vues de performances dynamiques, les tables et les vues de dictionnaire de données requises par l'agent. Il doit également disposer des autres privilèges sur les systèmes et objets Oracle nécessaires pour exécuter certaines commandes de base de données.

Procédure

1. (Facultatif) S'il n'existe pas d'ID utilisateur de base de données, créez-en un à l'aide des fonctions Oracle en exécutant la commande suivante : `create user` *`nom_utilisateur`* `identified by` *`mot_de_passe`*
2. Accordez à l'ID utilisateur Oracle créé en exécutant le script **`krzgrant.sql`** fourni avec Agent Oracle Database, des privilèges de sélection sur les vues de performances dynamiques, les tables et les vues de dictionnaire de données. Cette étape doit être effectuée préalablement à la configuration de l'agent. Pour consulter les instructions de personnalisation et d'exécution du script **`krzgrant.sql`**, voir «Personnalisation du script krzgrant.sql» et «Exécution du script **`krzgrant.sql`**», à la page 587.

   Remarque : Les privilèges de sélection sur les vues de performances dynamiques, les tables et les vues de dictionnaire de données dépendent des capacités de la base de données Oracle dans des environnements d'application spécifiques. Vous pouvez accorder des privilèges Oracle autorisés à l'ID utilisateur de base de données Oracle uniquement pour les vues de performances dynamiques, les tables et les vues de dictionnaire de données utilisées par Agent Oracle Database.
3. Accordez à l'ID utilisateur Oracle qu'utilise Agent Oracle Database d'autres privilèges d'objet Oracle et privilèges système en utilisant les fonctions Oracle.

Personnalisation du script krzgrant.sql :

Si vous ne voulez pas autoriser les privilèges de sélection autorisés Oracle sur certaines vues de performances dynamiques, tables et vues de dictionnaire de données dans le script **`krzgrant.sql`**, vous pouvez personnaliser le script avant de l'exécuter.

Remarque : L'instance d'agent vérifie tous les privilèges par défaut du script **`krzgrant.sql`** et fait état d'un événement d'agent signalant un manque de privilèges lors du démarrage de l'agent. Vous pouvez désactiver la vérification des privilèges en utilisant le paramètre de variable suivant : KRZ_CHECK_ORACLE_PRIVILEGE=FALSE. L'étape de test de connexion de la configuration de l'interface graphique vérifie l'ensemble des privilèges Oracle définis dans le fichier `krzgrant.sql`. Si vous confirmez que l'utilisateur Oracle dispose bien des privilèges adéquats, ignorez l'échec de vérification des privilèges lors de l'étape de test de connexion.

Modifiez le fichier `krzgrant.sql` dans un éditeur de texte en clair pour supprimer ou ajouter le préfixe '--' au début des instructions d'attribution de droits afin d'éviter l'exécution d'attribution de privilèges pour les vues et les tables Oracle non autorisées.

Par exemple, remplacez les lignes suivantes :

```
execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

par ces lignes :

```
-- execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
-- execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
-- execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
-- execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
-- execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

Attribution de privilèges aux utilisateurs non SYS pour les instances ASM

Vous devez vous connecter aux instances ASM qui utilisent les rôles SYSDBA et SYSASM pour les utilisateurs. Si vous ne souhaitez pas utiliser le compte SYS pour vous connecter aux instances ASM, créez un compte utilisateur et attribuez les rôles SYSDBA et SYSASM au compte.

Procédure

1. Exécutez les commandes suivantes pour créer un compte utilisateur et attribuer des rôles :
   - Connectez-vous à la base de données ASM avec le rôle SYSASM afin de créer un utilisateur pour un agent et lui accorder le rôle SYSDBA ou SYSASM :
     a. `create user` *`nom_utilisateur`* `identified by` *`mot_de_passe`*
     b. `grant sysdba to` *`nom_utilisateur`*

        `and`

        `grant sysasm to` *`nom_utilisateur`*
2. Lors de la création de la connexion ASM dans la fenêtre de configuration, indiquez l'utilisateur *UserName* et le rôle SYSDBA ou SYSASM.

   Remarque : Si vous choisissez le rôle SYSASM pour accéder à la base de données ASM, vous devez configurer l'instance d'agent en utilisant le répertoire de base Oracle ou le répertoire client Oracle Instant pour vous connecter à la base de données Oracle.

Exécution du script `krzgrant.sql` :
Avant de commencer

- Si vous n'exécutez pas le script **`krzgrant.sql`**, un événement est généré dans l'espace de travail des événements d'agent.
- Pour effectuer la procédure d'installation, voir Chapitre 9, «Installation des agents», à la page 161.

Après l'installation, le script **`krzgrant.sql`** se trouve dans le répertoire suivant :

- Windows *`rép_install`*`\TMAITM6_X64`
- Linux AIX *`rép_install/architecture`*`/rz/bin`

où :

rép_install
Répertoire d'installation de l'Agent Oracle Database.

architecture
Identificateur de l'architecture système d'IBM Application Performance Management ou de Cloud APM. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *`rép_install`*`/registry/archdsc.tbl`.

Le script **`krzgrant.sql`** est utilisé comme suit : `krzgrant.sql` *`ID_utilisateur répertoire_temporaire`*

où :

ID_utilisateur
ID de l'utilisateur Oracle. Doit être créé avant l'exécution de ce ficher SQL. Exemple de valeur : *tivoli*.

Répertoire_temporaire
Nom du répertoire temporaire destiné à recevoir le fichier de sortie `krzagent.log` du script **`krzgrant.sql`**. Ce répertoire doit exister avant que vous n'exécutiez ce script SQL. Par exemple : `rép_install/tmp`.

Vous devez disposer du rôle d'autorisation d'administrateur de la base de données Oracle et du droit en écriture sur le répertoire temporaire pour effectuer la procédure qui suit.

Procédure

1. Dans la ligne de commande, exécutez les commandes de définition des variables d'environnement.
   - Windows
     ```
     SET ORACLE_SID= sid
     SET ORACLE_HOME= home
     ```
   - Linux AIX
     ```
     ORACLE_SID = sid
     export ORACLE_SID
     ORACLE_HOME = home
     export ORACLE_HOME
     ```

   où :

   sid Identificateur du système Oracle, sensible à la casse.

   home Répertoire de base de l'instance Oracle surveillée.
2. A partir de la fenêtre de ligne de commande utilisée pour définir les variables d'environnement, démarrez Oracle SQL Plus ou un autre outil de lancement d'instructions SQL.
3. Connectez-vous à la base de données Oracle en tant qu'utilisateur Oracle disposant des privilèges administrateur.
4. Accédez au répertoire contenant le script **`krzgrant.sql`** et exécutez la commande suivante pour attribuer les privilèges de sélection :

   `@krzgrant.sql ID_utilisateur répertoire_temporaire`

   Le résultat est consigné dans le fichier `krzagent.log` du répertoire temporaire. Ce journal enregistre les vues et les tables pour lesquelles l'agent Agent Oracle Database a reçu les privilèges de sélection.

   Une fois les privilèges accordés, vous pouvez configurer et démarrer l'Agent Oracle Database.

Configuration de la surveillance du système d'exploitation

Les agents Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS et Monitoring Agent for Windows OS sont configurés automatiquement. Toutefois, vous pouvez configurer la surveillance des fichiers journaux pour les agents de système d'exploitation afin de pouvoir surveiller les fichiers journaux d'application. Vous pouvez également installer les agents de système d'exploitation en tant qu'utilisateur non superutilisateur.

Exécution des agents de système d'exploitation en tant qu'utilisateur non superutilisateur

Vous pouvez exécuter l'Monitoring Agent for Windows OS, l'Monitoring Agent for UNIX OS et l'Monitoring Agent for Linux OS en tant qu'utilisateur non superutilisateur.

Pour exécuter l'agent Windows OS en tant qu'utilisateur non superutilisateur, voir «Exécution de Monitoring Agent for Windows OS en tant qu'utilisateur non superutilisateur», à la page 589.

Pour exécuter l'Monitoring Agent for UNIX OS et l'Monitoring Agent for Linux OS en tant qu'utilisateur non superutilisateur, voir «Démarrage d'agents en tant qu'utilisateur non superutilisateur», à la page 1039.

Exécution de Monitoring Agent for Windows OS en tant qu'utilisateur non superutilisateur

Vous pouvez exécuter l'agent Windows OS en tant qu'utilisateur non superutilisateur, mais certaines fonctions ne sont pas disponibles.

Lorsque vous exécutez l'agent Windows OS en tant qu'utilisateur non superutilisateur, certaines fonctions ne sont pas disponibles dans les groupes d'attributs suivants si elles sont la propriété exclusive du compte administrateur :

- Registre
- Tendance de fichier
- Modification de fichier

Le déploiement à distance d'autres agents n'est pas disponible car des droits d'administrateur sont nécessaires pour installer les nouveaux agents.

Pour Agent Management Services, le programme de surveillance ne peut pas arrêter ni démarrer d'agent pour lequel il ne dispose pas des droits appropriés.

Pour créer un utilisateur non superutilisateur, créez un utilisateur limité (non superutilisateur) et attribuez-lui des droits sur le registre, comme dans l'exemple suivant :

- Accès complet à `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`
- Accès en lecture à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`

L'utilisateur qui démarre l'Monitoring Agent for Windows OS – Service principal doit disposer des droits nécessaires pour gérer l'Monitoring Agent for Windows OS - Service de surveillance. Celui qui démarre l'Monitoring Agent for Windows OS – Service de surveillance doit également disposer des droits nécessaires pour gérer tous les services administrés par Agent Management Services, notamment l'Monitoring Agent for Windows OS - Service principal. Pour accorder à des utilisateurs les droits de gestion des services système dans Windows, utilisez les modèles de sécurité et la stratégie de groupe, ou éditez le fichier `Subinacl.exe`. Pour plus d'informations, reportez-vous à la documentation Microsoft à l'adresse suivante : http://support.microsoft.com/kb/325349(http://support.microsoft.com/kb/325349).

L'exemple suivant montre comment accorder à des utilisateurs les droits de gestion des services système à l'aide des modèles de sécurité :

1. Cliquez sur **Démarrer** > **Exécuter**, puis entrez `mmc` dans la zone Ouvrir et cliquez sur **OK**.
2. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Cliquez sur **Ajouter** > **Configuration et analyse de la sécurité**, puis cliquez de nouveau sur **Ajouter**.
4. Cliquez sur **Fermer** puis sur **OK**.
5. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur **Configuration et analyse de la sécurité**, puis sur **Ouvrir une base de données**.
6. Indiquez un nom et un emplacement pour la base de données, puis cliquez sur **Ouvrir**.
7. Dans la boîte de dialogue Importer un modèle qui s'affiche, cliquez sur le modèle de sécurité que vous souhaitez importer, puis sur **Ouvrir**.
8. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur **Configuration et analyse de la sécurité**, puis sur **Analyser l'ordinateur maintenant**.
9. Dans la boîte de dialogue Effectuer l'analyse qui s'affiche, acceptez le chemin par défaut du fichier journal qui s'inscrit dans la zone du chemin du fichier journal des erreurs. Vous pouvez aussi indiquer un autre emplacement. Cliquez sur **OK**.

10. Une fois l'analyse terminée, configurez les autorisations pour le service comme suit :
    a. Dans l'arborescence de la console, cliquez sur **Services système**.
    b. Dans le panneau de droite, cliquez deux fois sur Monitoring Agent for Windows OS - Service principal.
    c. Sélectionnez la case à cocher **Définir cette règle dans la base de données**, puis cliquez sur **Modifier la sécurité**.
    d. Pour configurer des autorisations pour un nouvel utilisateur ou un nouveau groupe, cliquez sur **Ajouter**.
    e. Dans la boîte de dialogue Sélectionner les utilisateurs, les ordinateurs ou les groupes, saisissez le nom de l'utilisateur ou du groupe pour lequel vous souhaitez définir des autorisations, puis cliquez sur **OK**. Dans la liste Autorisations par utilisateur et groupe, sélectionnez la case à cocher **Autoriser** (à côté de **Démarrer**). L'autorisation d'arrêt et d'interruption étant sélectionnée par défaut, l'utilisateur ou le groupe a toute latitude pour démarrer, arrêter ou interrompre le service.
    f. Cliquez sur **OK** deux fois.
11. Répétez l'étape 10 pour configurer les autorisation de service de l'Monitoring Agent for Windows OS - Service de surveillance.
12. Pour appliquer les nouveaux paramètres de sécurité à l'ordinateur local, cliquez avec le bouton droit de la souris sur **Configuration et analyse de la sécurité**, puis cliquez sur **Configurer l'ordinateur maintenant**.

Remarque : Vous pouvez utiliser également l'outil de ligne de commande Secedit pour configurer et analyser la sécurité du système. Pour plus d'informations sur Secedit, cliquez sur **Démarrer** > **Exécuter**, puis entrez `cmd` et cliquez sur **OK**. A l'invite de commande, entrez `secedit /?`, puis appuyez sur la touche **ENTREE**. Lorsque vous appliquez des paramètres à l'aide de cette méthode, tous les paramètres du modèle sont réappliqués. Il est possible que cette méthode redéfinisse certaines autorisations de fichier, registre ou service précédemment configurées.

L'exemple suivant montre comment définir l'Monitoring Agent for Windows OS et les services de surveillance pour la connexion en tant qu'utilisateur non superutilisateur à l'aide de la console Windows Services :

1. Cliquez sur **Démarrer** > **Exécuter**, puis entrez `services.msc` et cliquez sur **OK**.
2. Sélectionnez **Monitoring Agent for Windows OS - Service principal**.
3. Cliquez avec le bouton droit de la souris sur **Propriétés**.
4. Vérifiez que le type de démarrage est réglé sur Automatique.
5. Sélectionnez l'onglet **Ouvrir une session**, puis **Ouvrir une session en tant que "Ce compte"** et entrez l'ID et le mot de passe. Cliquez sur **OK**.
6. Sélectionnez **Monitoring Agent for Windows OS - Programme de surveillance**.
7. Cliquez avec le bouton droit de la souris sur **Propriétés**.
8. Vérifiez que le type de démarrage est réglé sur Manuel.
9. Sélectionnez l'onglet **Ouvrir une session**, puis **Ouvrir une session en tant que "Ce compte"** et entrez l'ID et le mot de passe. Cliquez sur **OK**.

Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation

Les agents Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS et Monitoring Agent for Windows OS sont configurés automatiquement. Toutefois, vous pouvez configurer la surveillance des fichiers journaux pour les agents de système d'exploitation afin de pouvoir surveiller les fichiers journaux d'application.

Une fois filtrées par les agents, les données sont envoyées sous forme d'un événement de journal à la console console Cloud APM.

Ajout ou suppression de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation

Vous pouvez ajouter la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation afin de permettre à ces derniers de filtrer les données des fichiers journaux. Vous pouvez ensuite, le cas échéant, supprimer la configuration de la surveillance des fichiers journaux pour les agents de système d'exploitation.

Avant de commencer

Les agents de système d'exploitation incluent désormais un exemple de fichier regex1.conf et de fichier regex1.fmt que vous pouvez consulter avant de configurer les fichiers .conf et .fmt. Ces fichiers se trouvent ici :

- Sous UNIX/LINUX : `<rép_install>/samples/logfile-monitoring`
- Sous Windows : `<rép_install\samples\logfile-monitoring`

A l'aide d'un éditeur de texte, créez un fichier de configuration `.conf` et un fichier de format `.fmt`. Pour plus d'informations sur le contenu de ces fichiers, voir «Fichier de configuration», à la page 596 et «Fichier de format», à la page 606. Vous devez veiller à sauvegarder ces fichiers sur le système à partir duquel vous accédez à la console Performance Management, de sorte que vous puissiez les télécharger sur le serveur Cloud APM.

Pourquoi et quand exécuter cette tâche

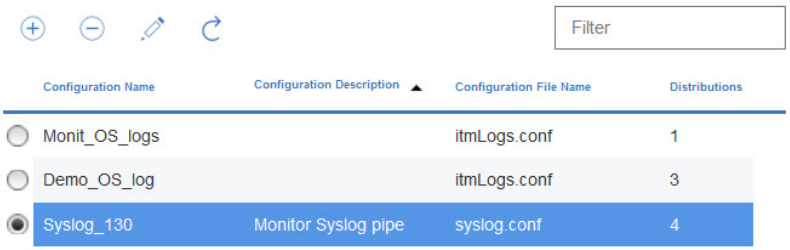
Pour permettre aux agents du système d'exploitation de surveiller les fichiers journaux, vous devez télécharger le fichier de configuration et le fichier de format, et préciser à quel agent de système d'exploitation la configuration s'applique. L'agent de système d'exploitation reçoit par téléchargement les fichiers `.conf` et `.fmt` et surveille les fichiers journaux indiqués dans la configuration.

Procédure

Ajout de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation

1. Cliquez sur **Configuration du système** > **Configuration d'agent**.
2. En fonction du système où vous souhaitez surveiller les fichiers journaux, cliquez sur l'onglet **Système d'exploitation Unix**, **Système d'exploitation Linux** ou **Système d'exploitation Windows**.
3. Pour créer une configuration, cliquez sur l'icône (+) pour ouvrir la fenêtre New Log File Configuration. Entrez un nom et une description de la configuration.
4. Pour afficher le contenu des fichiers `.conf` et `.fmt`, cliquez sur **Visualiser**.
5. Pour transférer la configuration à l'aide du serveur Cloud APM, sélectionnez le fichier `.conf` et le fichier `.fmt` sur le système où vous ouvrez la console Performance Management et cliquez sur **Terminé**.
6. Dans l'onglet de l'agent de système d'exploitation, sélectionnez la configuration que vous envoyez par téléchargement.

   Important : Les fichiers `.conf` et `.fmt` qui sont distribués aux agents sont renommés en utilisant le nom de configuration que vous définissez.



7. Pour déployer la configuration, dans la table **Log Configuration Distributions List**, sélectionnez les agents vers lesquels vous souhaitez déployer la configuration et cliquez sur **Appliquer les modifications**.

Suppression de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation

8. Sélectionnez le nom de configuration.
9. Supprimez les systèmes gérés et cliquez sur **Appliquer les modifications**.

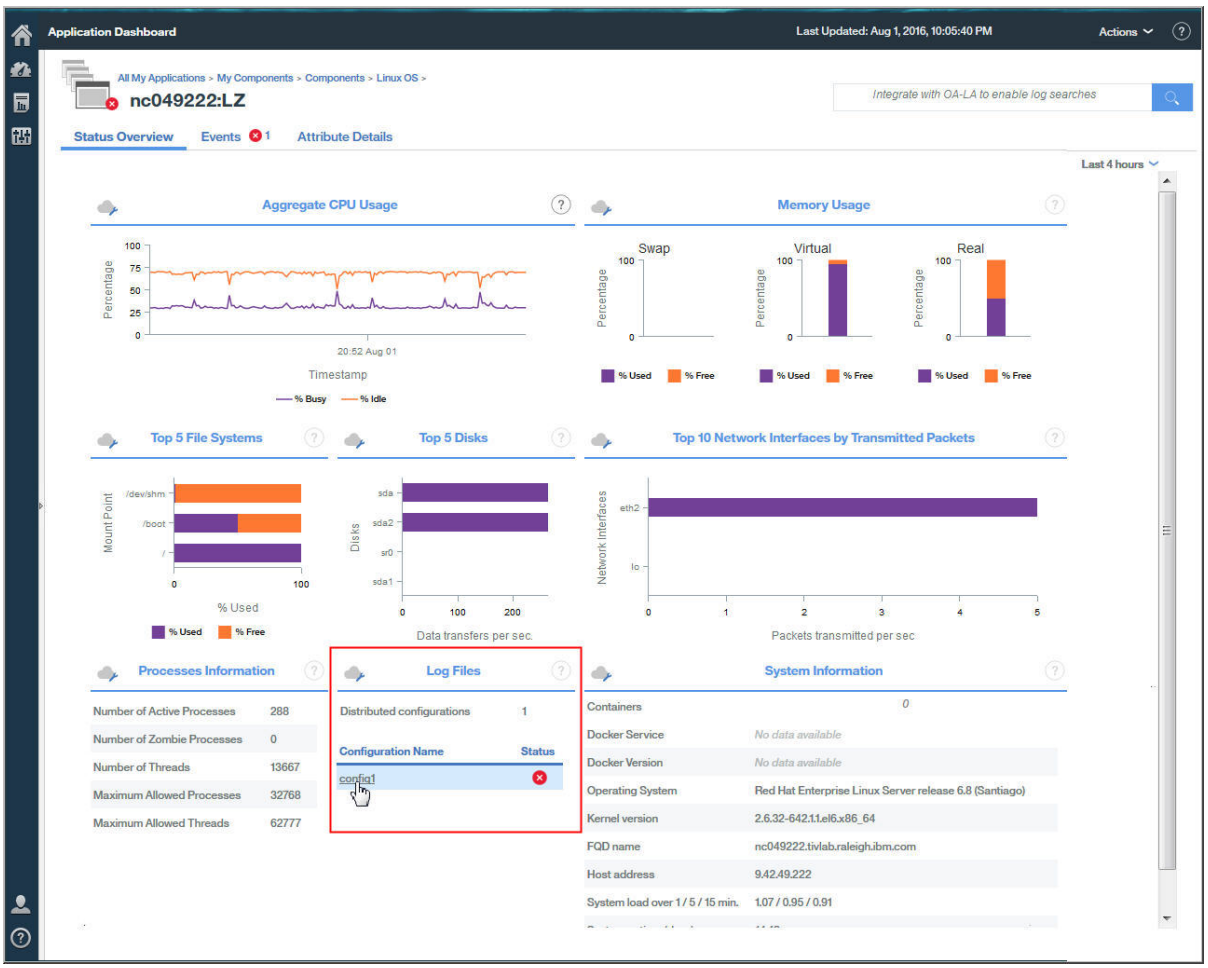
   Important :
   Une fois que vous avez supprimé la configuration de la surveillance des fichiers journaux, la ressource de surveillance correspondante est conservée et reste en ligne jusqu'au redémarrage de l'agent de système d'exploitation. Les ressources de surveillance des fichiers journaux hors ligne sont supprimées une fois écoulé le délai indiqué dans l'option **Délai avant suppression d'un système hors ligne**.

Affichage du contenu de surveillance du fichier journal

Vous pouvez afficher la configuration de surveillance du fichier journal pour les agents de système d'exploitation déployés pour surveiller les fichiers journaux.

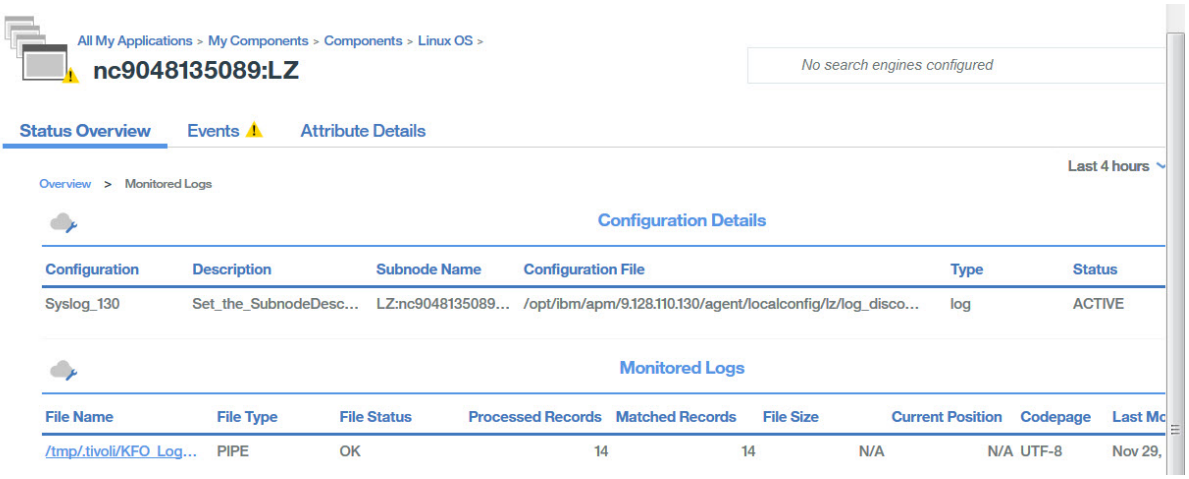
Procédure

1. Cliquez sur **Performance** > **Tableau de bord de performance d'application**, puis sélectionnez une application incluant l'agent de système d'exploitation où vous avez déployé la configuration de surveillance des fichiers journaux.
2. Descendez dans la hiérarchie jusqu'au tableau de bord de l'agent de système d'exploitation puis dans le widget Fichiers journaux, cliquez sur le profil pour afficher les configurations de surveillance des journaux distribuées et les journaux surveillés.

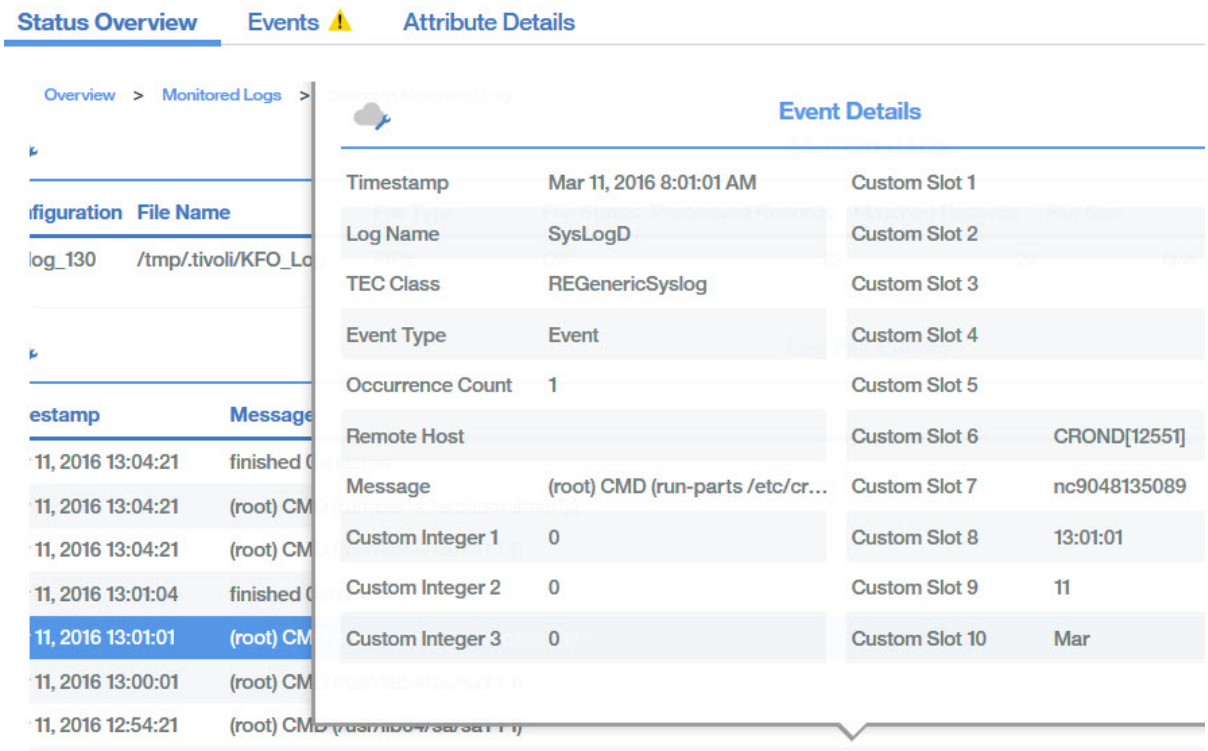


Les informations de configuration incluent le nom de la configuration, la description associée, le sous-noeud, le fichier de configuration, le statut et le code d'erreur.

3. Cliquez sur le nom du fichier journal pour afficher tous les événements de fichier journal qui sont associés au fichier journal.



4. Cliquez sur l'événement pour afficher les détails associés, par exemple toutes les zones définies dans le fichier de format.



Affichage des événements de surveillance des fichiers journaux

Après avoir configuré l'agent de système d'exploitation pour surveiller les fichiers journaux des applications, vous pouvez créer des seuils afin de déclencher des alarmes sur les conditions de fichier journal dont vous souhaitez être alerté.

Procédure

1. Dans la barre de navigation, cliquez sur l'icône **Configuration système** > **Gestionnaire de seuils**.
2. Sélectionnez le système d'exploitation cible pour **Type de source de données**.
3. Cliquez sur Ajouter pour créer un seuil.
4. Définissez une gravité pour l'événement qui dépasse ce seuil.
5. Sélectionnez le jeu de données pour lequel vous souhaitez créer un seuil. Les jeux de données suivants sont admissibles pour la surveillance des fichiers journaux :
   - K*pp* : statistiques RegEx des fichiers journaux
   - K*pp* : statut des fichiers journaux
   - K*pp* : événements de profil des fichiers journaux
6. Cliquez sur **Ajouter** pour ajouter une condition. Dans la zone **Ajouter une condition**, sélectionnez un attribut et un opérateur, puis entrez une valeur de seuil.

   Au besoin, répétez cette procédure pour ajouter d'autres conditions à votre seuil.
7. Dans la section Affectation de groupes, sélectionnez le groupe de ressources auquel vous souhaitez affecter le seuil.
8. Cliquez sur **Sauvegarder**.
9. Dans la barre de navigation, cliquez sur l'icône **Configuration système** > **Configuration avancée**.
10. Dans la catégorie **Intégration d'UI**, définissez la valeur **Activer les événements sous-noeud** sur True.
11. Cliquez sur **Sauvegarder**.

Résultats

Lorsque la condition indiquée a la valeur true, l'événement de fichier journal qui déclenche l'alerte apparaît dans l'onglet Evénements.

Variables d'environnement de la surveillance des fichiers journaux

Vous pouvez définir des variables d'environnement pour la surveillance des fichiers journaux dans les fichiers d'environnement de l'agent de système d'exploitation.

Définissez les variables d'environnement ci-dessous et remplacez K*PC* par le code de l'agent de système d'exploitation, où *PC* est le code d'agent de deux caractères, par exemple, klz est le code de l'agent de système d'exploitation Linux.

K*PC*_FCP_LOG
Cette variable est disponible dans le fichier *rép_install*/config/.*pc*.environment. La valeur par défaut est True et permet d'activer ou de désactiver la fonction de surveillance des journaux.

K*PC*_FCP_LOG_PROCESS_MAX_CPU_PCT
Ce paramètre est le pourcentage maximal autorisé de toutes les unités centrales système utilisées par l'agent au cours d'une minute. Les valeurs admises sont comprises entre 5 et 100. La valeur par défaut est 100. Ce paramètre est associé à la fonctionnalité de régulation de l'UC. Si vous définissez une valeur inférieure à 5, la valeur minimale de 5 est utilisée.

K*PC*_FCP_LOG_PROCESS_PRIORITY_CLASS
Ce paramètre définit la priorité du planificateur du système d'exploitation pour le processus. A est la priorité la plus faible, C la valeur par défaut du système d'exploitation et F la priorité la plus haute. Le paramètre est l'une des valeurs suivantes : A, B, C, D, E, F. Ces valeurs sont remplacées par toutes les valeurs que vous indiquez dans le fichier .conf.

K*PC*_FCP_LOG_SEND_EVENTS
Le paramètre par défaut est True et est utilisé par l'agent de système d'exploitation pour envoyer des événements au serveur Cloud APM.

K*PC*_FCP_LOG_SEND_EIF_EVENTS
Le paramètre par défaut est True. Si ce paramètre a pour valeur Yes, l'agent envoie les données d'événement au serveur Cloud APM ou à un récepteur EIF tel que la sonde OMNIbus EIF. Si ce paramètre a pour valeur No, l'agent n'envoie pas les données d'événement. La définition de ce paramètre est globale et s'applique à l'ensemble des profils de surveillance.

Remarque : Le récepteur EIF consomme des événements. Sinon, des problèmes peuvent se produire lorsque les données s'accumulent dans le cache de l'agent.

K*PC*_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN
Les agents de système d'exploitation qui surveillent les événements des fichiers journaux présentent une limitation de sous-noeud. Pour gérer les événements des fichiers journaux, le nom de système géré (MSN) du sous-noeud possède la structure suivante : UX:*NOMHOTECITRA_NOMPROFIL*. La longueur maximale du nom de sous-noeud est 32 caractères. Si le nom de système géré de sous-noeud généré dépasse cette longueur, il est tronqué à 32 caractères. Il correspond à la sous-chaîne extraite du nom du profil.

Dans le fichier de configuration de l'agent de système d'exploitation, utilisez les variables suivantes pour gérer les noms de profil trop longs :

- Agent de système d'exploitation UNIX : KUX_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Agent de système d'exploitation Linux : KLZ_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Agent de système d'exploitation Windows : KNT_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true

Par exemple, si vous avez un agent appelé `aixhost_nc123456789A` de 20 caractères, `CTIRAHOSTNAME=aixhost_nc123456789A` comprend 20 caractères.

Si vous avez deux profils appelés :

```
ProfileLong12A (14 caractères)
ProfileLong12B (14 caractères)
```

les noms de systèmes gérés de sous-noeud associés suivants sont attendus :

```
UX:aixhost_nc123456789A_ProfileLong12A (38 caractères)
UX:aixhost_nc123456789A_ProfileLong12B (38 caractères)
```

Toutefois, les noms de systèmes gérés de sous-noeud sont tronqués à 32 caractères et les noms effectifs sont les mêmes pour les deux :

```
UX:aixhost_nc123456789A_ProfileL
UX:aixhost_nc123456789A_ProfileL
```

Pour tronquer CTIRAHOSTNAME au lieu du nom de profil, définissez la variable *Kpc_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true*.

Ainsi, si *n* est la longueur du nom de profil, disons 14, la sous-chaîne du nom de système géré liée à *CTIRAHOSTNAME* est tronquée à partir de 32-n-3 caractères. La variable *CTIRAHOSTNAME* est donc la suivante : `aixhost_nc1234`. Les noms de systèmes gérés de sous-noeud distinctifs sont alors :

```
UX:aixhost_nc1234_ProfileLong12A
UX:aixhost_nc1234_ProfileLong12B
```

Fichier de configuration

Les agents de système d'exploitation utilisent un fichier de configuration qui est lu par l'agent à son démarrage. Le fichier contient des options de configuration et des filtres. Vous devez créer ce fichier de configuration, puis configurer l'instance d'agent afin qu'elle l'utilise.

L'horodatage du fichier de configuration est surveillé toutes les 60 secondes. Si l'horodatage du fichier change, l'agent réinitialise sa configuration de manière dynamique sans redémarrer. Pour plus d'informations, voir «Modification des fichiers de configuration et de format de l'agent», à la page 610.

Le fichier `.conf` de l'agent de système d'exploitation accepte les options suivantes :

codepage
Page de codes du fichier surveillé. Utilisez ce paramètre dans le fichier de configuration lorsque la page de codes du fichier surveillé est différente de celle du système. Indiquez la page de codes du fichier surveillé, par exemple ibm-5348_P100-1997, UTF-16 ou UTF-8.

ConfigFilesAreUTF8=Y
Ce paramètre indique que le fichier de configuration et le fichier de format sont au format UTF-8. Utilisez ce paramètre si le codage des fichiers de configuration est UTF-8 et que la page de codes du système ne l'est pas. L'agent prend en charge le codage système (valeur par défaut).

DupDetectionKeyAttributes
Liste d'attributs Cloud APM séparés par des virgules et utilisés pour identifier les événements en double. Si tous les attributs nommés sont identiques dans deux événements, ces deux événements sont considérés comme des doublons. Cette option s'applique uniquement aux événements. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1049.

Remarque :

1. Les noms d'attribut sont sensibles à la casse. Vous devez donc entrer le nom exactement comme décrit.
2. Si vous ne spécifiez pas de liste d'attributs, les valeurs sont définies sur `Class` et `Logname` par défaut.

ENFORCE_STRICT_TEC_COMPATIBILITY

Ce paramètre fait référence à tous les caractères espaces figurant dans les données du journal pour s'assurer que les caractères sont respectés. Par exemple, lorsque vous utilisez le format `"%s %s"` pour extraire des informations de messages de journal, l'agent de système d'exploitation recherche non seulement un espace littéral mais également tout autre espace existant, comme des tabulations ou des retours chariot.

Lorsque ce paramètre n'est pas défini, le comportement par défaut de l'agent de système d'exploitation lors de la recherche d'une chaîne de format de style Tivoli Enterprise Console consiste à rechercher autant de texte d'entrée que possible en traitant le format de gauche à droite.

Par exemple, pour la chaîne de format `%s:%s` et la chaîne d'entrée `one:two:three`, l'agent de système d'exploitation affecte `un.deux` au premier paramètre (correspondant au premier caractère `%s`) et `trois` au second paramètre.

Remarque :

1. Ce paramètre ne s'applique pas aux instructions de format qui utilisent la syntaxe d'expression régulière.
2. La définition de ce paramètre a un impact sur les performances. Pour améliorer le comportement et les performances du processus de mise en correspondance, évitez de définir ce paramètre et utilisez des expressions régulières à la place.

EventSummaryInterval

Indique la durée en secondes pendant laquelle l'agent recherche des événements en double à supprimer. Définissez ce paramètre à un entier positif. Cette option s'applique uniquement aux événements. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1049.

EventFloodThreshold

Indique quels événements sont envoyés lorsque le système détecte des doublons parmi les événements. La valeur de ce paramètre est `send_none`, `send_all`, `send_first` ou un entier positif. Cette option s'applique uniquement aux événements. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1049.

EventMaxSize

Taille en octets maximale d'un événement généré. Si vous le spécifiez, ce paramètre est utilisé à deux endroits :

1. Le paramètre peut être utilisé par l'agent afin de définir la taille de la mémoire tampon utilisée pour le traitement des événements. S'il n'est pas défini, cette mémoire tampon a par défaut une taille de 16384 octets. Si la taille de la mémoire tampon est insuffisante, les événements sont tronqués et risquent d'être supprimés.
2. Le paramètre peut être utilisé par l'émetteur EIF afin de définir la taille de la mémoire tampon utilisée pour l'envoi des événements à un récepteur EIF (tel que la sonde OMNIbus EIF). S'il n'est pas défini, cette mémoire tampon a par défaut une taille de 4096 octets. Si la taille de la mémoire tampon est insuffisante, les événements sont supprimés.

FileComparisonMode

Indique quels fichiers journaux sont surveillés lorsque plusieurs fichiers journaux correspondent à un modèle générique. Les valeurs suivantes sont disponibles :

CompareByAllMatches

Cette valeur est le comportement par défaut. Tous les fichiers correspondant au modèle générique spécifié dans le paramètre `LogSources` sont surveillés.

CompareByLastUpdate

Parmi les fichiers correspondant au masque indiqué dans le paramètre `LogSources`, le fichier dont l'horodatage de mise à jour est le plus récent est surveillé.

CompareBySize
Si au moins deux fichiers correspondent aux critères de modèle de nom de fichier spécifiés, seul le fichier le plus volumineux est surveillé. N'utilisez pas la valeur `CompareBySize` avec des fichiers correspondants multiples qui sont mis à jour en même temps et dont la taille de fichier augmente. Si le fichier le plus volumineux est soumis à des changements fréquents, la surveillance risque de redémarrer indéfiniment au début du nouveau fichier sélectionné. Dans le cas de correspondances multiples où un seul fichier est actif et mis à jour à la fois, utilisez plutôt la valeur `CompareBySize`.

CompareByCreationTime
Parmi les fichiers correspondant au masque indiqué dans le paramètre `LogSources`, le fichier dont l'horodatage de création est le plus récent est surveillé. Cette valeur est soumise aux restrictions suivantes :

- La valeur ne concerne que les systèmes d'exploitation Windows car les systèmes d'exploitation UNIX et Linux n'enregistrent pas l'heure de création effective des fichiers.
- La valeur n'est pas prise en charge pour les fichiers distants surveillés par le biais du protocole SFTP/SSH (Secure Shell File Transfer Protocol).

Conseil : Les valeurs `CompareByLastUpdate`, `CompareBySize` et `CompareByCreationTime` peuvent toutes être utilisées pour la rotation des fichiers journaux. `CompareByLastUpdate` est généralement utilisé pour ces fichiers.

FQDomain
Indique si l'agent a défini un nom de domaine et la manière dont il l'a défini :

- Si ce paramètre a pour valeur `yes`, l'agent détermine le nom de domaine.
- Si ce paramètre a pour valeur `no`, l'agent ne définit pas le nom de domaine. L'attribut `fqhostname` comporte une chaîne vide.
- Si ce paramètre n'a pas pour valeur `yes` ou `no`, le système accepte le nom de domaine comme valeur et l'ajoute au nom d'hôte.

Pour plus d'informations, voir «Fichier de format», à la page 606.

IncludeEIFEventAttr
L'agent inclut un attribut volumineux appelé *EIFEvent*, qui correspond à une représentation de l'événement envoyé via la fonction EIF si cette fonction est activée. Les informations contenues dans l'attribut *EIFEvent* peuvent également se trouver dans d'autres attributs. Sa taille élevée étant problématique, il est désactivé par défaut. Indiquez la valeur `y` pour réactiver l'attribut EIFEvent.

Remarque : L'utilisation de cet attribut risque d'entraîner l'échec des seuils si les événements sont volumineux. Dans ce contexte, un événement volumineux désigne un événement où le nombre total d'octets nécessaires pour contenir l'ensemble des valeurs, des attributs et de leurs noms représente une chaîne de plus de 3600 octets.

LognameIsBasename
Lorsque vous indiquez `y`, la valeur de l'attribut `Logname` est le nom de base du fichier journal où l'événement a été détecté. Cette option s'applique uniquement aux événements Performance Management. Le chemin est supprimé. Par exemple, `/data/logs/journal.log` devient `journal.log`. Si ce paramètre a pour valeur `n`, le chemin complet est indiqué. L'attribut étant limité à 64 caractères, le nom sera donc tronqué s'il est plus long. Pour cette raison, la valeur par défaut est `y`. Pour visualiser le chemin complet dans un attribut plus long, vous pouvez l'indiquer dans la section de mappages dans un format du fichier`.fmt`, par exemple `filename FILENAME CustomSlot1`. Le mappage complète l'attribut nommé `filename` avec le chemin complet du fichier dans lequel l'événement a été détecté et le mappe à l'entrée `CustomSlot1` de 256 caractères.

LogSources
Indique les fichiers journaux texte à interroger pour les messages. Le chemin d'accès complet de chaque fichier doit être spécifié et les noms de fichier doivent être séparés par des virgules. Dans

chaque nom de fichier, vous pouvez également utiliser un astérisque (*) pour représenter une séquence de caractères ou un point d'interrogation (?) pour représenter un caractère seul. Par exemple, `journal*` renvoie tous les fichiers journaux dont le nom commence par le mot `journal` alors que `journal???` renvoie tous les fichiers journaux dont le nom inclut `journal` suivi de trois caractères. Ces caractères génériques ne s'appliquent qu'au nom de fichier ; vous devez spécifier le chemin de manière explicite.

Si vous souhaitez utiliser des expressions régulières ou la correspondance de modèles dans le chemin, voir la description du paramètre RegexLogSources.

Une source de fichier journal n'a pas besoin d'exister lorsque l'agent est démarré ; le fichier journal est interrogé lors de sa création.

NewFilePollInterval
Indique la fréquence en secondes à laquelle l'agent vérifie les nouveaux fichiers à surveiller. Par exemple, supposons qu'un nom de fichier indiqué dans le paramètre *LogSources* ou *RegexLogSources* du fichier de configuration n'existe pas encore. Lorsque l'agent démarre, il vérifie à nouveau l'existence des fichiers à l'issue de cet intervalle.

NumEventsToCatchUp
Indique l'événement à partir duquel l'agent démarre dans le journal. Ce paramètre offre une certaine flexibilité si la source surveillée est nouvelle ou que l'agent est arrêté pour une période prolongée. Les valeurs suivantes sont valides :

Remarque : Pour les fichiers texte, les valeurs `0` et `-1` s'appliquent. Pour le journal des événements Windows, les valeurs `0`, `-1` et `n` s'appliquent.

0 Démarre au niveau de l'événement suivant des journaux. Cette valeur est la valeur par défaut.

-1 Lorsque le paramètre a pour valeur `-1`, l'agent enregistre sa position dans le fichier surveillé. Si l'agent est arrêté et redémarré plus tard, il pourra ainsi traiter tous les événements consignés dans le journal pendant son arrêt. En l'absence de ce paramètre, l'agent ignore les événements qui se sont produits alors qu'il était arrêté et redémarre à partir de la fin du fichier. Ce paramètre ne s'applique ni aux canaux, ni à la surveillance de syslog sur les systèmes UNIX et Linux.

n La valeur est un entier positif. L'agent démarre à partir du *nième* événement par rapport à l'événement le plus récent consigné dans les journaux. Autrement dit, il démarre *n* événements avant l'événement le plus récent consigné dans les journaux. Si *n* est supérieur au nombre d'événements disponibles, tous les événements disponibles sont traités.

Remarque : Vous pouvez utiliser la valeur `n` uniquement avec le journal d'événements Windows. Le système ignore la valeur `n` lorsque le paramètre `UseNewEventLogAPI` est défini sur *y*.

PollInterval
Indique la fréquence en secondes à laquelle le système interroge chaque fichier journal spécifié dans le paramètre `LogSources` au sujet des nouveaux messages. La valeur par défaut est `5` secondes.

Si vous avez mis à jour un adaptateur de journal des événements Windows à partir d'une version précédente et que le paramètre `PollingInterval` est défini sur une valeur dans le registre Windows, vous devez définir le paramètre `PollInterval` sur la même valeur dans le fichier de configuration de l'agent Windows. Cette règle s'applique uniquement si vous remplacez un agent de système d'exploitation Tivoli Enterprise Console qui avaient des valeurs dans le registre.

ProcessPriorityClass

Définit la priorité de processus pour l'agent. Vous pouvez ajuster cette valeur afin d'améliorer les performances système lorsque l'agent traite de grands volumes d'événements et sollicite trop de ressources processeur. Les valeurs admises sont :

- `A` - Priorité très faible
- `B` - Priorité faible
- `C` - Priorité moyenne
- `D` - Priorité moyenne haute
- `E` - Priorité élevée
- `F` - Priorité très élevée
- `USE_CONF_FILE_VALUE` - La valeur indiquée dans le fichier de configuration est utilisée. Cette valeur est la valeur par défaut.

RegexLogSources

Indique les fichiers journaux texte à interroger pour les messages. Ce paramètre est identique au paramètre LogSources, à ceci près que les métacaractères d'expression régulière peuvent être utilisés dans la partie nom de base du nom de fichier et dans un sous-répertoire du nom de fichier. Il offre plus de flexibilité que le paramètre LogSources, car il permet de décrire plusieurs fichiers à surveiller dans plusieurs répertoires.

Par exemple, la définition de `/var/log/mylog*` pour l'instruction LogSources est comparable à l'utilisation du métacaractère point `(.)` suivi du métacaractère astérisque `(*)` pour former `/var/log/mylog.*` dans l'instruction RegexLogSources. Dans cet exemple, le système interroge tous les fichiers journaux du répertoire `/var/log` dont le nom de base commence par le mot `journal` suivi de zéro caractère ou plus. Avec la chaîne `/var/log/journal.+`, le système interroge tous les fichiers journaux du répertoire `/var/log` dont le nom de base commence par le mot `journal` suivi d'un caractère ou plus.

A l'instar de LogSources, le chemin d'accès complet de chaque fichier doit être spécifié et les noms de fichier doivent être séparés par des virgules. Notez toutefois que les virgules sont des caractères valides dans les expressions régulières. Pour établir une distinction entre une virgule utilisée dans une expression régulière et une virgule utilisée pour séparer des noms de fichier, les virgules utilisées dans une expression régulière doivent être associées au caractère d'échappement barre oblique inversée `(\)`.

Par exemple, si vous souhaitez rechercher des journaux correspondant à l'une des expressions régulières `/logs/.*\.log` et `/other/logs/[a-z]{0,3}\.log`, vous devez associer la clause `{0,3}` de la seconde expression au caractère d'échappement afin que l'agent ne la considère pas comme le début d'une nouvelle expression : `RegexLogSources=/logs/.*\.log,/other/logs/[a-z]{0\,3}\ .log`

Si des métacaractères sont utilisés dans le nom de chemin, ils ne peuvent être utilisés que dans un seul sous-répertoire du chemin. Par exemple, vous pouvez spécifier `/var/log/[0-9\.]*/ journal.*` pour avoir des métacaractères dans un sous-répertoire. La chaîne `[0-9\.]*` fait correspondre les sous-répertoire de `/var/log` comportant uniquement des chiffres et des points `(.)`. La chaîne `mylog.*` fait correspondre les noms des fichiers des sous répertoires `/var/log` qui commencent par le mot `journal` et suivis de zéro caractère ou plus.

Etant donné que certains systèmes d'exploitation utilisent la barre oblique inversée `(\)` comme séparateur de répertoire, il peut être confondu avec un métacaractère d'échappement d'expression régulière. Pour éviter cette confusion, des barres obliques doivent toujours être utilisées pour désigner des répertoires. Par exemple, les fichiers Windows qui sont spécifiés sous la forme `C:\temp\mylog. *` peuvent signifier que le `\t` est un caractère de tabulation abrégé. Par conséquent, utilisez toujours des barres obliques `(/)` comme séparateurs de répertoire sur tous les systèmes d'exploitation. Par exemple, `C:/temp/mylog.*` représente tous les fichiers du répertoire `C:/temp` qui commencent par `mylog`.

Si plusieurs sous-répertoires contiennent des métacaractères, un message de trace est également généré. Par exemple, `c:/[0-9\.]*/temp.files/journal.*` inclut deux sous-répertoires qui contiennent des métacaractères. `[0-9\.]*` est le premier sous-répertoire défini avec des métacaractères et `temp.files` est le deuxième sous-répertoire qui utilise le métacaractère point (`.`). Dans ce cas, l'agent considère que le premier sous-répertoire défini avec le métacaractère est utilisé et que les répertoires suivants possédant des métacaractères sont ignorés.

SubnodeName
Valeur de chaîne pouvant être utilisée pour remplacer le nom par défaut affecté à un sous-noeud de profil de surveillance. Par défaut, le nom de sous-noeud affecté à un profil de surveillance correspond au nom de base du fichier de configuration utilisé pour ce profil. En utilisant ce paramètre, il est possible d'affecter un nom de sous-noeud différent.

SubnodeDescription
Valeur de chaîne pouvant être utilisée pour affecter une valeur à l'attribut *Subnode Description* de *LFAProfiles*.

UnmatchLog
Permet d'indiquer un fichier dans lequel sont consignés les événements supprimés qui ne peuvent pas être analysés dans une classe d'événement par l'agent. Les événements supprimés peuvent ensuite être analysés pour déterminer si le format de fichier de l'agent doit faire l'objet de modifications. Les événements correspondant à un masque qui utilise *DISCARD* n'apparaissent pas dans le journal de non correspondance, car ils correspondent à un masque.

Cette option est utilisée dans un environnement de test pour valider les filtres dans le fichier de format. Elle peut entraîner la saturation de votre système de fichiers si vous la conservez pendant des périodes prolongées.

Options pour la surveillance à distance des fichiers via le protocole SSH

A part **SshHostList**, qui est une liste, tous les paramètres ne peuvent avoir qu'une seule valeur, qui est appliquée à tous les hôtes distants spécifiés dans **SshHostList**.

Seuls les fichiers journaux texte sont pris en charge. Le rapport d'erreur AIX, syslog et le journal des événements Windows ne sont pas pris en charge.

Conseil : Vous pouvez configurer syslog pour placer sa sortie dans un fichier journal, puis surveiller à distance ce fichier texte avec l'agent de système d'exploitation.

SshAuthType
Doit avoir pour valeur *PASSWORD* ou *PUBLICKEY*. Si ce paramètre a pour valeur *PASSWORD*, la valeur de **SshPassword** est considérée comme le mot de passe à utiliser pour l'authentification SSH avec tous les systèmes distants. S'il a pour valeur *PUBLICKEY*, la valeur de **SshPassword** est considérée comme la phrase de passe qui contrôle l'accès au fichier de clés privées. Si ce paramètre a pour valeur *PUBLICKEY*, **SshPrivKeyfile** et **SshPubKeyfile** doivent également être indiqués.

SshHostList
Liste séparée par des virgules des hôtes distants à surveiller. Tous les fichiers journaux spécifiés dans les instructions **LogSources** ou **RegexLogSources** sont surveillés sur chacun des hôtes figurant dans cette liste. Si l'un des noms d'hôte indiqués est *localhost*, l'agent surveille le même ensemble de fichiers directement sur le système local. Lorsque vous indiquez *localhost*, le protocole SSH n'est pas utilisé pour accéder aux fichiers sur le système local ; les fichiers journaux sont lus directement.

SshPassword
Lorsque la valeur de **SshAuthType** est *PASSWORD*, cette valeur correspond au mot de passe du compte de l'utilisateur spécifié dans **SshUserid**. Vous pouvez indiquer le mot de passe du compte sous la forme d'un texte en clair ou indiquer un mot de passe chiffré à l'aide de la commande

CLI IBM Tivoli Monitoring **itmpwdsnmp**. Pour savoir comment procéder pour chiffrer un mot de passe à l'aide de la commande **itmpwdsnmp**, voir «Surveillance des fichiers journaux distants : Chiffrement d'un mot de passe ou d'une phrase de passe», à la page 616.

Lorsque la valeur de **SshAuthType** est *PUBLICKEY*, cette valeur correspond à la phrase de passe qui permet de déchiffrer la clé privée spécifiée par le paramètre **SshPrivKeyfile**. Vous pouvez indiquer la phrase de passe sous la forme d'un texte en clair ou indiquer une phrase de passe chiffrée à l'aide de la commande CLI IBM Tivoli Monitoring **itmpwdsnmp**. Pour savoir comment procéder pour chiffrer un mot de passe à l'aide de la commande **itmpwdsnmp**, voir «Surveillance des fichiers journaux distants : Chiffrement d'un mot de passe ou d'une phrase de passe», à la page 616.

Remarque : Si la valeur de **SshAuthType** est *PUBLICKEY* et que vous avez configuré SSH afin qu'aucune phrase de passe ne soit nécessaire, **SshPassword** doit avoir pour valeur NULL. Pour associer **SshPassword** à la valeur NULL, l'entrée du fichier de configuration est :

```
SshPassword=
```

SshPort
Port TCP auquel se connecter pour utiliser SSH. Si ce paramètre n'est pas défini, il prend par défaut la valeur *22*.

SshPrivKeyfile
Si **SshAuthType** a pour valeur *PUBLICKEY*, cette valeur doit correspondre au chemin complet du fichier contenant la clé privée de l'utilisateur indiqué dans **SshUserid**, et **SshPubKeyfile** doit également être défini. Si **SshAuthType** n'a pas pour valeur *PUBLICKEY*, cette valeur n'est pas nécessaire et elle est ignorée.

SshPubKeyfile
Si **SshAuthType** a pour valeur *PUBLICKEY*, cette valeur doit correspondre au chemin complet du fichier contenant la clé publique de l'utilisateur indiqué dans **SshUserid**, et **SshPrivKeyfile** doit également être défini. Si **SshAuthType** n'a pas pour valeur *PUBLICKEY*, cette valeur n'est pas nécessaire et elle est ignorée.

SshUserid
Nom d'utilisateur sur des systèmes distants que l'agent utilise pour l'authentification SSH.

Linux AIX

Option prise en charge sur les systèmes UNIX et Linux uniquement

AutoInitSyslog
Si cette option a pour valeur `Yes`, l'agent configure automatiquement l'utilitaire syslog pour consigner un ensemble standard d'événements dans un canal surveillé par l'agent. En l'activant, vous pouvez surveiller les événements syslog sans être obligé de gérer et remettre à zéro les fichiers journaux. Si cette option n'est pas définie dans le fichier de configuration, cela revient à utiliser la valeur `No`.

Restriction : Cette option n'est pas prise en charge pour la surveillance du fichier journal à distance.

Windows

Options prises en charge sur les systèmes Windows uniquement

NTEventLogMaxReadBytes
Si vous utilisez l'ancienne interface du journal des événements NT (`UseNewEventLogAPI` non défini sur `y`) pour lire les données du journal des événements sur un système Windows, l'agent lit les données jusqu'à ce nombre d'octets chaque fois qu'il vérifie la présence de nouvelles données dans le journal des événements. Si ce paramètre a pour valeur `0`, l'agent essaie de lire toutes les nouvelles données comme il le faisait dans les versions antérieures. Cette activité peut solliciter l'agent pendant longtemps si le système comporte un grand volume d'événements. La valeur par

défaut est 655360. Si vous définissez ce paramètre, il se peut que l'agent ne s'arrête pas exactement à la valeur indiquée, mais plutôt vers le multiple le plus proche de la taille de la mémoire tampon interne par rapport à cette valeur.

PreFilter
Indique la façon dont les événements d'un journal d'événements Windows sont filtrés avant le traitement par l'agent. Les instructions PreFilter sont utilisées par PreFilterMode au moment où les filtres déterminent quels événements du journal des événements doivent être envoyés à l'agent. Un événement correspond à une instruction PreFilter lorsque chaque spécification *attribut=valeur* de l'instruction PreFilter correspond à un événement du journal d'événements. Une instruction PreFilter doit contenir au moins la spécification de journal et peut comporter jusqu'à trois spécifications supplémentaires (toutes facultatives) : l'ID d'événement, le type d'événement et la source d'événement. L'ordre des attributs dans l'instruction importe peu.

Le format de l'instruction PreFilter est le suivant :

```
PreFilter:Log=log_name;EventId=value; EventType=value;Source=value;
```

Vous pouvez indiquer plusieurs valeurs pour chaque attribut en les séparant par des virgules.

Chaque instruction PreFilter doit se trouver sur une ligne distincte.

Le paramètre PreFilter n'est pas obligatoire. Tous les événements du journal d'événements Windows sont envoyés à l'agent si aucun préfiltre n'est spécifié et que le paramètre PreFilterMode=OUT est utilisé.

PreFilterMode
Ce paramètre s'applique uniquement au journal d'événements Windows. Il permet de spécifier si les événements du journal des événements Windows correspondant à une instruction PreFilter sont envoyés (PreFilterMode=IN) ou ignorés (PreFilterMode=OUT). Les valeurs admises sont IN, in, OUT et out. La valeur par défaut est OUT.

Le paramètre PreFilterMode est facultatif. S'il n'est pas spécifié, seuls les événements ne correspondant à aucune instruction PreFilter sont envoyés à l'agent.

Remarque : Si vous définissez le paramètre PreFilterMode=IN, vous devez également définir les instructions PreFilter.

SpaceReplacement
Ce paramètre correspond par défaut à TRUE pour le journal d'événements Windows (Windows Server 2008 uniquement mais par pour les versions précédentes du journal des événements. Lorsque le paramètre SpaceReplacement a pour valeur TRUE, tous les espaces figurant dans les zones security ID, subsource, Level et keywords des messages du journal d'événements sont remplacés par des traits de soulignement (_). Lorsque le paramètre SpaceReplacement a pour valeur FALSE, tous les espaces figurant dans les zones security ID, subsource, Level et keywords des messages du journal d'événements sont conservés. Pour plus d'informations sur ce paramètre, voir «Journal des événements Windows», à la page 1051.

UseNewEventLogAPI
Lorsque ce paramètre a pour valeur y sur les systèmes Windows, l'agent utilise la nouvelle interface de journal d'événements Windows pour analyser les journaux d'événements. Le paramètre est pris en charge sur les systèmes Windows 2008 et version ultérieure uniquement. Il permet d'accéder à la plupart des nouveaux journaux d'événements débutés dans Windows 2008, ainsi qu'aux applications qui s'exécutent dessus. Ce paramètre est ignoré sur les versions antérieures de Windows et sur les systèmes UNIX et Linux. Pour plus d'informations sur ce paramètre, voir «Journal des événements Windows», à la page 1051.

WINEVENTLOGS
Permet de contrôler quels journaux d'événements Windows sont contrôlés.

L'instruction WINEVENTLOGS est une liste délimitée par des virgules, sans espaces. Pour plus d'informations, voir «Journal des événements Windows», à la page 1051.

Remarque : Les retours chariot, tabulations ou nouvelles lignes figurant dans les événements Windows sont remplacés par des espaces.

AIX

Option prise en charge sur les systèmes AIX uniquement

AIXErrptCmd

Permet d'indiquer une chaîne de commande **errpt** (rapport d'erreur) qui sera exécutée par l'agent. Le résultat de la commande est importé dans le flux de données de journal faisant l'objet d'une surveillance.

Dans l'exemple de commande ci-dessous, l'agent recherche la chaîne *mmjjhhmmaa* et la remplace par la date et l'heure de démarrage. Seule la première occurrence de la chaîne est remplacée.

```
AIXErrptCmd=errpt -c -smmddhhmmyy
```

Bien que vous puissiez indiquer votre propre commande `errpt`, vous devez utiliser l'option `-c` (mode simultané) afin que la commande s'exécute en continu. Vous ne pouvez pas utiliser l'option `-t`, ni les options suivantes qui donnent lieu à la sortie détaillée : `-a`, `-A` ou `-g`.Le flux de données est le résultat standard de la commande `errpt`. Par conséquent, les expressions régulières du fichier `.fmt` doivent être écrites de telle sorte qu'elles correspondent. Par exemple, la commande pourrait renvoyer la sortie de données suivante :

```
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
F7FA22C9   0723182911 I O SYSJ2      UNABLE TO ALLOCATE SPACE IN FILE SYSTEM
2B4F5CAB   1006152710 U U ffdc       UNDETERMINED ERROR
2B4F5CAB   1006152610 U U ffdc       UNDETERMINED ERROR
```

Exemple de format qui utilise les lignes de données, mais pas l'en-tête :

```
REGEX GenericErrpt
^([A-F0-9]{8}) +([0-9]{10}) ([A-Z]) ([A-Z]) (\S+) +(.*)$
Identifier $1 CustomSlot1
Timestamp  $2 CustomSlot2
T          $3 CustomSlot3
C          $4 CustomSlot4
Resource   $5 CustomSlot5
msg        $6
END
```

Pour plus d'informations, voir *Monitoring an AIX Binary Log* dans le Guide d'utilisation d'IBM Agent Builder.

Options qui s'appliquent uniquement lorsque des événements sont transmis à un récepteur EIF

Important : Ces options sont applicables à des événements EIF envoyés directement à Operations Analytics - Log Analysis, OMNIbus ou tout autre récepteur générique EIF. Elles ne sont pas destinées à être utilisées avec le serveur Cloud APM.

BufferEvents

Indique comment le stockage temporaire d'événements est activé. Les valeurs admises sont :

- **YES** - Stocke les événements dans le fichier spécifié par le paramètre BufEvtPath (valeur par défaut).
- **MEMORY_ONLY** - Stocke les événements dans une mémoire temporaire.
- **NO** - Ne stocke pas les événements dans une mémoire permanente ou temporaire.

BufEvtPath

Indique le chemin d'accès complet du fichier cache de l'agent. Si ce chemin d'accès n'est pas rectifié, la valeur par défaut est :

- AIX `/etc/Tivoli/tec/cache`
- Windows `\etc\Tivoli\tec\cache`

Remarque : Si des événements sont transmis à plusieurs serveurs, vous devez spécifier une valeur *BufEvtPath* pour chaque canal de transmission. Un numéro d'index est ajouté au nom *BufEvtPath* de chaque entrée supplémentaire. Par exemple, utilisez le paramètre *BufEvtPath1* pour préciser le nom de chemin du fichier cache de l'agent aux fins de transmission vers le premier serveur supplémentaire. La valeur définie pour chaque paramètre *BufEvtPath* doit être unique.

BufEvtMaxSize
Indique la taille maximale en kilo-octets du fichier cache de l'agent. La valeur par défaut est 64. Lorsque le paramètre *BufferEvents* a pour valeur Yes, le fichier cache stocke les événements sur le disque. La taille minimale pour le fichier est 8 ko. Le système ignore toutes les tailles de fichier inférieures et utilise à la place la valeur 8 ko. Il n'existe pas de limite supérieure pour la valeur que vous avez spécifiée pour la taille maximale du fichier.

Remarque : Si le fichier cache existe déjà, vous devez supprimer le fichier afin de prendre en compte vos modifications.

NO_UTF8_CONVERSION
Indique si Event Integration Facility (EIF) encode les données d'événement au format UTF-8. Lorsque vous associez ce paramètre à `YES`, Event Integration Facility n'encode pas les données d'événement au format UTF-8. Le système suppose que les données ont déjà un encodage UTF-8 lorsqu'elles sont transmises à Event Integration Facility. Toutefois, un préfixe est ajouté à l'indicateur pour signaler que les données possèdent un encodage in UTF-8 (si l'indicateur n'existe pas au début des données d'événement). La valeur par défaut est `NO`.

MaxEventQueueDepth
Spécifie le nombre maximal d'événements pouvant être placés en file d'attente à des fins de transmission. Lorsque la limite est atteinte, chaque nouvel événement placé dans la file d'attente supplante l'événement le plus ancien dans la file d'attente. Si vous ne définissez pas ce paramètre, la valeur par défaut est 1 000. Ce paramètre s'applique à l'ensemble des canaux de transmission si *NumAdditionalServers* est utilisé.

NumAdditionalServers
Cette entrée est nécessaire si vous souhaitez transmettre des événement à plusieurs systèmes ObjectServer Netcool/OMNIbus. Il permet d'indiquer le nombre de serveurs auxquels les événements sont transmis. Les valeurs admises sont comprises entre 1 et 8.

ServerLocation
Indique le nom de l'hôte sur lequel le serveur d'événements est installé. Indiquez le nom de hôte ou l'adresse IP. Utilisez le format à points pour l'adresse IP. Si vous le souhaitez, vous pouvez indiquer des valeurs de reprise en ligne pour les emplacements du serveur, telles que `ServerLocation1=2.3.4.5.2.3.4.6` ; si vous indiquez des valeurs pour *ServerLocation*, vous devez également indiquer une valeur *ServerPort* supplémentaire pour chaque *ServerLocation*.

Remarque : Si des événements sont transmis à plusieurs serveurs, vous devez indiquer une valeur *ServerLocation* pour chaque serveur. Un numéro d'index est ajouté au nom *ServerLocation* de chaque entrée supplémentaire. Par exemple, utilisez *ServerLocation1* pour spécifier le nom de l'hôte sur lequel le premier serveur supplémentaire est installé.

ServerPort
Indique le numéro de port sur lequel le récepteur EIF écoute les événements. Le paramètre *ServerPort* peut contenir jusqu'à huit valeurs, séparées par des virgules. Si vous indiquez des valeurs de basculement pour le paramètre *ServerLocation*, vous devez définir une valeur *ServerPort* équivalente. ServerPort n'est pas utilisé lorsque le paramètre *TransportList* est indiqué.

Remarque : Si des événements sont transmis à plusieurs serveurs, vous devez spécifier une valeur *ServerPort* pour chaque serveur. Un numéro d'index est ajouté au nom *ServerPort* de chaque entrée supplémentaire. Par exemple, utilisez *ServerPort1* afin d'indiquer le numéro de port sur lequel le récepteur EIF écoute les événements pour le premier serveur supplémentaire.

TransportList

Indique les noms définis par l'utilisateur des mécanismes de transport, séparés par des virgules. Lorsqu'un mécanisme de transport échoue pour des applications expéditrices, l'API utilise les mécanismes de transport suivants dans l'ordre indiqué dans la liste. Pour les applications réceptrices, l'API crée et utilise tous les mécanismes de transport. Le type et le canal de transport de chaque *nom_type* doivent être spécifiés au moyen des mots clés Type et Channels :

***nom_type*Type**

Indique le type de transport du mécanisme de transport défini par le paramètre *TransportList*. SOCKET est le seul type de transport pris en charge.

Le serveur et le port de chaque nom_canal sont indiqués par les paramètres *ServerLocation* et *ServerPort*.

***nom_type*Channels**

***nom_canal*Port**
Indique le numéro de port sur lequel le serveur de mécanismes de transport écoute le canal indiqué (indiqué par le paramètre *Channel*). Lorsque ce mot clé a pour valeur zéro, l'associateur de port est utilisé. Ce mot clé est obligatoire.

***nom_canal*PortMapper**
Active l'associateur de port pour le canal indiqué.

***nom_canal*PortMapperName**
Si l'associateur de port est activé, indique le nom de l'associateur de port.

***nom_canal*PortMapperNumber**
Indique l'ID enregistré par l'appel de procédure distante (RPC).

***nom_canal*PortMapperVersion**
Si l'associateur de port est activé, indique la version de l'associateur de port.

***nom_canal*ServerLocation**
Indique le nom du serveur d'événements et de la région sur laquelle le serveur de mécanismes de transport se trouve pour le canal indiqué. Le canal est défini par le paramètre *Channel*. Ce mot clé est obligatoire.

Le fichier de configuration EIF accepte les options EIF génériques lorsqu'il est utilisé directement avec OMNIbus. Ces options fonctionnent uniquement sur une connexion EIF avec OMNIbus. Ils n'affectent pas les événements qui sont envoyés au serveur Cloud APM. Pour plus d'informations sur ces options EIF, voir EIF keywords.

Fichier de format

Les agents de système d'exploitation extraient les messages des journaux système, puis établissent une concordance entre différents messages de journal à des classes d'événement. Pour effectuer cette association, ils utilisent un fichier de format comme fichier de recherche pour déterminer quelle classe d'événement ils doivent lire, sur quoi effectuer la correspondance et la manière de formater les données.

Lorsque le fichier de format est utilisé comme fichier de recherche, le système compare toutes les spécifications de format figurant dans le fichier en commençant par le début du fichier. Si deux classes correspondent ou qu'il existe plusieurs classes correspondantes pour un message, le système utilise la première expression qu'il trouve à partir de la fin du fichier. Si aucune correspondance n'est trouvée, l'événement est supprimé. Un événement supprimé est consigné dans le journal de non correspondance s'il est défini dans le fichier `.conf`.

La syntaxe d'expression régulière permettant de créer des masques pour établir des correspondances entre les messages de journal et des événements est décrite. Le filtrage d'expression régulière est pris en charge via des bibliothèques ICU (International Components for Unicode) pour vérifier si une valeur d'attribut examinée correspond ou non au modèle indiqué.

Pour plus d'informations sur l'utilisation d'expressions régulières, visitez la page sur les expressions régulières dans le document *ICU User Guide*.

Spécifications du fichier de format :

Le fichier de format décrit les modèles que l'agent recherche pour faire correspondre des événements dans les journaux surveillés. Il se compose d'une ou de plusieurs spécifications de format.

Vous pouvez modifier le fichier de format pendant qu'une instance d'agent est en cours d'exécution. L'agent lit le fichier au démarrage et surveille son horodatage toutes les 60 secondes. Si l'horodatage du fichier change, l'agent réinitialise sa configuration de manière dynamique sans redémarrer. Pour plus d'informations, voir «Modification des fichiers de configuration et de format de l'agent», à la page 610.

Si vous créez de nouveaux modèles pour faire correspondre un événement, utilisez la nouvelle syntaxe d'expression régulière. Elle se compose des éléments suivants :

- En-tête de format
- Expression régulière
- Mappages d'attribut
- Instruction End

L'en-tête de format contient le mot clé **REGEX**, qui indique à l'agent que vous utilisez une expression régulière pour rechercher une correspondance au modèle dans le journal surveillé.

Vous affectez cette expression régulière à une classe d'événement comme indiqué dans l'exemple suivant :

```
REGEX REExample
```

Si vous utilisez la classe d'événement spéciale prédéfinie `*DISCARD*` comme classe d'événement, tous les enregistrements de journal correspondant au modèle associé sont supprimés et aucun événement n'est généré pour eux. Par exemple :

```
REGEX *DISCARD*
```

Lorsque le système a trouvé une correspondance, il ne consigne aucune donnée dans le journal de non concordance. Les correspondances d'enregistrements de statut du fichier journal incluent ces événements supprimés.

Remarque : Vous pouvez affecter plusieurs définitions d'événement soit à la même classe d'événement, soit à différentes classes d'événement. Le nom de classe est arbitraire ; vous pouvez l'utiliser pour spécifier le type d'événement ou regrouper des événements de différentes manières.

Placé en-dessous de l'en-tête de format, le contenu de format se compose d'une expression régulière sur la première ligne et de mappages. Chaque mappage figure sur une ligne distincte (voir exemple suivant).

Toutes les lignes correspondant aux expressions régulières sont sélectionnées et envoyées au serveur de surveillance en tant qu'événements. L'expression régulière contient des sous-expressions. Celles-ci vous permettent d'associer certaines parties spécifiques de ces lignes qui sont identiques à une variable appelée *attribut* (slot) dans la fonction d'intégration d'événements (EIF).

Le journal de surveillance illustré ici contient trois lignes que vous pouvez surveiller :

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

Par exemple, supposons que vous générez un événement pour une erreur spécifique, telle que les lignes commençant par `Error` et que vous ignorez les lignes commençant par `Warning`. L'expression régulière doit correspondre aux lignes commençant par `Error` et doit également comporter une sous-expression. La

sous-expression est placée entre parenthèses et doit uniquement correspondre au texte de saisie que vous souhaitez affecter à l'attribut *msg*. La définition de format ci-dessous est une expression régulière simple composée d'une seule sous-expression :

```
REGEX REExample
Error: (.*)
msg $1
END
```

En fonction de cette spécification de format et de l'ensemble de données de journal précédent, l'agent génère deux événements. La classe d'événement `REEXample` est affectée à ces deux événements. Dans le premier événement, la valeur `disk failure` est affectée à l'attribut *msg*. De la même manière, la valeur out of memory est affectée à l'attribut *msg* dans le second événement. Comme la ligne `Warning` ne correspond pas à l'expression régulière, le système l'ignore et ne génère aucun événement.

Lorsque vous affectez la valeur $1 à l'attribut *msg*, vous lui affectez la valeur de la première sous-expression.

Si le journal a consigné les erreurs suivantes, vous pouvez affecter ces messages d'erreur à leur propre classe d'événement afin que le système vous informe immédiatement en cas de panne de disque :

```
Error: disk failure on device /dev/sd0: bad sector
Error: disk failure on device /dev/sd1: temperature out of range
```

Vous pouvez inclure une description du disque sur lequel l'erreur s'est produite et détailler plus précisément l'erreur de disque dans l'événement.

L'expression régulière suivante contient deux sous-expressions qui identifient ces informations :

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Vous affectez ces deux sous-expressions à des attributs d'événement. Les deux événements générés contiennent les valeurs suivantes :

```
"device=/dev/sd0" and "msg=bad sector"
"device=/dev/sd1" and "msg=temperature out of range"
```

Si vous utilisez la fonction d'intégration d'événements pour générer le premier événement, elle s'affiche comme indiqué dans l'exemple suivant :

```
DiskError;device='/dev/sd0';msg='bad sector';END
```

Si l'événement est envoyé au serveur Cloud APM, l'attribut nommé *msg* est affecté à l'attribut d'agent Performance Management qui porte le même nom. Mais l'attribut *device* ne comporte pas d'attribut prédéfini.

Si vous devez visualiser la valeur affectée à *device* directement dans la console Cloud APM ou créer des seuils associés, vous devez l'affecter à un attribut Performance Management.

L'agent de système d'exploitation inclut les treize attributs prédéfinis suivants :

- Dix attributs de type chaîne allant de *CustomSlot1* à *CustomSlot10*
- Trois attributs de type entier allant de *CustomInteger1* à *CustomInteger3*

L'utilisation de ces noms d'attribut dans le fichier de format entraîne la définition des attributs Performance Management qui portent le même nom. L'utilisation de ces attributs n'affecte pas le contenu de l'événement EIF envoyé directement à OMNIbus.

Remarque : Les noms d'attribut `CustomSlot` et `CustomInteger` sont sensibles à la casse. Vous devez donc entrer le nom exactement comme indiqué.

Vous affectez un attribut de la définition d'événement à l'un des ces attributs personnalisés Performance Management dans le fichier de format.

Vous affectez l'attribut *device* à l'attribut de type de chaîne Performance Management appelé *CustomSlot1*, comme indiqué dans l'exemple suivant :

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Lorsque l'événement s'affiche dans le Tableau de bord d'Application Performance, la valeur affectée à l'attribut *device* est affectée à l'attribut Performance Management appelé `CustomSlot1`. Vous pouvez afficher cette valeur dans la console Cloud APM ou l'utiliser pour définir des seuils. Vous pouvez affecter de la même manière n'importe quel attribut de la définition d'événement à l'un des dix attributs d'agent personnalisés en indiquant "`CustomSlot`*n*", où *n* est un nombre compris entre 1 à 10, à côté de la définition d'attribut.

Dans cet exemple, la première sous-expression est définie de manière spécifique sous la forme `(/dev/sd[0-9])`, mais la seconde sous-expression est définie de manière générale sous la forme `(.*)`. Lorsque vous définissez l'expression régulière de la manière la plus spécifique possible, vous améliorez les performances du système. Par conséquent, si vous entrez une recherche pour trouver une erreur sur une unité ne correspondant pas au message d'erreur spécifique défini ici, la procédure de recherche s'arrête immédiatement lorsque l'erreur est introuvable. Le système ne perd pas de temps à rechercher de correspondance.

Le mot clé *END* complète la spécification de format. L'en-tête de format, l'expression régulière et le mot clé *END* doivent commencer sur une nouvelle ligne comme indiqué dans l'exemple suivant :

```
REGEX REExample
Error:
msg $1
END <EOL>
<EOF>
```

Remarque : Pour le dernier format du fichier, vous devez insérer une nouvelle ligne après le mot clé **END** comme indiqué dans l'exemple. Sinon, le système générera une erreur d'analyse.

Les attributs entiers personnalisés *CustomInteger1* à *CustomInteger3* sont des attributs entiers 64 bits. Vous pouvez les utiliser de la même manière que les attributs chaînes `CustomSlot`. Vous pouvez utiliser ces attributs pour mapper des attributs ou des sous-expressions spécifiques du fichier journal à des attributs Cloud APM spécifiques. Comme ces attributs sont numériques, vous pouvez appliquer des comparaisons arithmétiques dessus (< et >, par exemple), ce qui n'est pas possible avec les attributs de chaîne.

Remarque : Bien que ces valeurs soient considérées comme des entiers par le serveur Cloud APM, elles sont toujours traitées comme des chaînes pour EIF et dans le fichier de format. Pour utiliser un attribut entier dans une instruction PRINTF, vous l'identifiez donc toujours sous la forme "%s" et non "%d".

L'exemple suivant illustre l'utilisation d'un attribut entier personnalisé. Supposons que le système reçoive un message UNIX syslog périodique indiquant le pourcentage d'espace libre sur le système de fichiers comme dans l'exemple d'enregistrement de journal suivant :

```
Oct 24 11:05:10 jimmy fschecker[2165]: Filesystem /usr is 97% full.
```

Vous pouvez utiliser l'instruction suivante dans le fichier de format pour vérifier le pourcentage d'espace libre sur le système de fichiers :

```
REGEX FileSystemUsage
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?):
Filesystem (.*?) is ([0-9]+)% full\.$
Month   $1 CustomSlot1
Date    $2 CustomSlot2
Time    $3 CustomSlot3
Host    $4 CustomSlot4
Service $5 CustomSlot5
Filesystem     $6 CustomSlot6
PctFull      $7  CustomInteger1
msg          PRINTF("%s: %s% full", Filesystem, PctFull)
END
```

Remarque : Dans l'instruction précédente, le code figurant entre les symboles ^ et $ sur les lignes 2 et 3 doit figurer sur une seule ligne.

Il se peut que d'autres événements insèrent des valeurs dans l'attribut *CustomInteger1*. Pour ne pas faire de confusion entre les différents types d'événement, vous pouvez utiliser la valeur de l'attribut *Class* pour limiter son effet au type d'événement approprié. Par exemple, la formule de seuil suivante entraîne le déclenchement du seuil uniquement lorsqu'un événement de la classe d'événement *FileSystemUsage* possède une valeur supérieure ou égale à 95 dans *CustomInteger1*:

```
(  Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Un événement peut ensuite utiliser *CustomInteger1* pour d'autres objectifs et ne pas dépasser ce seuil accidentellement.

En résumé, vous pouvez maintenant créer un seuil dans Performance Management qui utilise des opérateurs arithmétiques dans les attributs `CustomInteger`, ce qui n'est pas possible avec les attributs `CustomSlots`.

Remarque : Si vous mappez des données qui ne sont pas des entiers à l'attribut `CustomInteger`, la valeur obtenue peut être zéro (0) ou une valeur inattendue.

Modification des fichiers de configuration et de format de l'agent :

L'agent de système d'exploitation lit ses fichiers de configuration (`.conf`) et de format (`.fmt`) à son démarrage et surveille leur horodatage toutes les 60 secondes ensuite.

Si l'horodatage du fichier de configuration ou de format change, l'agent réinitialise sa configuration de manière dynamique sans redémarrer. Lors de la réinitialisation, la surveillance est interrompue momentanément. Lorsque la surveillance reprend, l'agent doit déterminer la position à partir de laquelle il doit redémarrer dans les journaux surveillés. L'agent se comporte donc de la même manière qu'un arrêt complet et un redémarrage.

Remarque : Lorsque l'agent se réinitialise après modification d'un fichier de configuration ou de format, le système réinitialise les informations des groupes d'attributs `Statistiques RegEx du fichier journal`, `Statut du fichier journal` et `Evénement de fichier journal`.

Par défaut, l'agent démarre la surveillance à partir de la fin du fichier à l'issue de la réinitialisation. Cette position de départ peut provoquer la disparition des événements qui se sont produits pendant l'interruption de la surveillance. Pour vous assurer que ces événements sont bien récupérés à la reprise de la surveillance, utilisez le paramètre `NumEventsToCatchUp=-1`.

L'utilisation du paramètre `NumEventsToCatchUp=-1` entraîne la gestion d'un fichier de position. Le fichier de position est mis à jour chaque fois que l'agent lit le fichier journal. Lors de la mise à jour, le système enregistre la position de l'agent dans le fichier journal dans l'éventualité d'un redémarrage de l'agent. La

gestion du fichier de position a un léger impact sur les performances système. Aussi, ne le gérez que lorsque c'est nécessaire. Pour plus d'informations sur `NumEventsToCatchUp`, voir «Fichier de configuration», à la page 596.

Remarque : Certaines valeurs de configuration ne sont pas présentes dans le fichier de configuration et sont définies lors de la configuration initiale. Si vous modifiez ces valeurs, vous devez redémarrer l'agent.

Héritage :

Les fichiers de format utilisent l'héritage pour déduire les définitions d'attribut à partir d'une spécification de format définie précédemment.

Utilisez la relation FOLLOWS pour créer des spécifications de format spécifiques à partir de spécifications de format génériques à l'aide de l'héritage.

Tout d'abord, définissez une classe de base que vous appellerez `DiskFailure`. Par exemple :

```
REGEX DiskFailure
Disk Failure on device (.*)
device $1 CustomSlot1
END
```

Cette expression régulière effectue une correspondance pour les erreurs `Disk Failure on device/dev/sd0` dans le journal de surveillance afin que la valeur `/dev/sd0` soit affectée à l'attribut *device* (unité).

Cependant, vous pouvez également voir une version longue de ce message d'erreur dans le journal de surveillance.

Par exemple, le message d'erreur `Disk Failure on device /dev/sd0, error code: 13` peut s'afficher.

Ce message d'erreur est mis en correspondance avec un attribut comme indiqué dans l'exemple suivant :

```
REGEX DiskFailureError FOLLOWS DiskFailure
Disk Failure on device (.*), error code: ([0-9]*)
errcode $2 CustomSlot2
END
```

Désormais, l'événement inclut les attributs *device* et *errcode*. Comme la classe d'événement `DiskFailure` a déjà défini un attribut pour le nom d'unité, vous permettez à la sous-classe d'hériter de cet attribut et cet héritage vous évite de le déclarer une seconde fois. L'attribut étant défini en tant que `$1`, le système affectera la première sous-expression de l'expression régulière à cet attribut.

Cependant, la classe `DiskFailureError` définit également une deuxième sous-expression. Vous pouvez affecter cette sous-expression à un nouvel attribut appelé `errcode` et le définir en tant que `$2` pour faire référence à la deuxième sous-expression de l'expression régulière. Ce type d'affectation est illustré dans l'exemple précédent qui présente un extrait du journal.

L'événement contient désormais l'attribut `device` qui est affecté de la valeur `/dev/sd0` et l'attribut `errcode` qui est affecté de la valeur 13. L'unité (device) est affectée à l'attribut CustomSlot1 tandis que le code d'erreur (errcode) est affecté à l'attribut CustomSlot2.

Les mappages d'attributs personnalisés Performance Management sont également hérités. Pour plus d'informations sur les mappages d'attributs personnalisés Performance Management, voir «Spécifications du fichier de format», à la page 607.

Multiligne :

La syntaxe multiligne permet de comparer les enregistrements occupant plusieurs lignes à des modèles dans le journal que vous surveillez.

Indiquez le caractère de retour à la ligne \n dans l'expression régulière pour indiquer où le retour à la ligne apparaît dans le journal de surveillance. L'exemple suivant illustre le type de syntaxe multiligne :

```
REGEX REMultiLine
Line1:(.*)\nLine2(.*)
msg $1
second_msg $2
END
```

Remarque : Windows Indiquez une combinaison de retours chariot \r\n et de nouvelles lignes.

Si les messages d'erreur suivants sont consignés dans le journal, l'événement REMultiLine est créé :

```
Line1: An error occurred
Line2: The error was "disk error"
```

La valeur `An error occurred` est affectée à l'attribut `msg` tandis que la valeur `The error was "disk error"` est affectée à l'attribut `second_msg`.

Mappages :

L'agent de système d'exploitation détermine la classe d'événement d'un message de journal système. Il détermine la classe d'événement en comparant le message à un masque dans le fichier de format.

L'agent convertit les messages de journal en instances de classe d'événement qui inclut les paires d'attributs `nom=valeur`. L'événement est ensuite envoyé au serveur d'événements.

L'agent détermine la classe d'événement d'un message de journal système à la source. Il détermine la classe d'événement en comparant le message de journal à un masque dans le fichier de format. Lorsque vous utilisez cette procédure de comparaison pour déterminer une classe, vous devez affecter des valeurs aux attributs.

Les valeurs d'attribut proviennent de différents endroits. Par exemple :

- Valeurs par défaut fournies par l'agent
- Entrées de journal correspondant à des sous-expressions spécifiques d'expressions régulières

Le fichier de format comporte une instruction de mappage qui respecte la syntaxe suivante :

```
nom    valeur CustomSlotn
```

Tout d'abord, vous spécifiez un identificateur pour décrire le `nom` d'un attribut (également appelé variable, emplacement ou identificateur de valeur). Ensuite, vous indiquez une valeur à affecter à cet attribut en utilisant l'une des valeurs décrites dans la section «Indicateurs de valeur», à la page 613.

Utilisez des attributs personnalisés pour afficher les données dans la console Performance Management et définir des seuils. Lorsque vous créez des seuils, toutes les valeurs d'attributs personnalisés sont des chaînes. Les attributs personnalisés sont également nécessaires au fonctionnement du mécanisme de détection des événements en double car vous devez identifier les attributs utilisés pour la détermination des doublons. Pour plus d'informations sur le filtrage d'événements, voir «Filtrage et récapitulatif des événements», à la page 1049. `msg` est un nom d'attribut spécial qui possède ses propres valeurs dans la table d'événements. Vous n'avez pas besoin d'utiliser d'attribut personnalisé pour `msg`.

Vous pouvez limiter la portée d'un attribut de façon à ce qu'il n'existe que dans la définition de format. Lorsque vous définissez l'attribut, vous devez faire précéder le nom d'attribut par un tiret. Par exemple :

```
-name valeur
```

Les attributs que vous définissez de cette façon ne sont pas inclus dans l'événement final. Cependant, vous pouvez faire référence à l'attribut à d'autres endroits dans la définition de format, notamment au sein d'une instruction `PRINTF`. Dans l'exemple `REGenericSyslog` suivant, l'attribut `service` n'est pas inclus

dans l'événement que vous générez, mais vous pouvez y faire référence dans l'instruction PRINTF. Il conserve la même valeur qui était appliquée à l'attribut d'origine lorsqu'il était spécifié sans tiret. Grâce à cette procédure, vous pouvez utiliser des variables temporaires de la définition de format qui ne sont pas incluses dans l'événement final. Par exemple, vous pouvez définir une classe d'événement REGenericSyslog pour comparer des événements UNIX syslog génériques de la manière suivante :

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?): (.*)$
month $1
date $2
time $3
host $4
-service $5
msg $6
syslog_msg PRINTF("service %s reports %s", service, msg)
END
```

Indicateurs de valeur :

Les mappages d'une spécification de format affectent des valeurs aux attributs.

La partie mappage d'une spécification de format comporte les types de spécificateur de valeur suivants :

- $i
- Constante de chaîne
- Instruction PRINTF

$i

L'attribut $i indique la position d'une sous-expression dans une chaîne de format. Chaque sous-expression est numérotée ; les numéros sont compris entre 1 et le nombre maximal de sous-expressions figurant dans la chaîne de format.

La valeur d'un indicateur de valeur $i (également appelé variable, emplacement ou attribut) correspond à la partie du message de journal système qui est rapprochée par la sous-expression correspondante.

Dans l'exemple suivant, l'agent Log File convertit un message de journal de l'utilitaire UNIX syslog en événement syslog comportant des valeurs définies :

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2})
 (.*?) (.*?): (.*)$
month   $1
date    $2
time    $3
host    $4
service $5
msg     $6
END
```

Chaque sous-expression numérotée de $1 à $6 correspond à un élément entre parenthèses de l'expression régulière.

L'événement syslog suivant :

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

a donc les valeurs suivantes :

```
month=Apr
date=6
time=10:03:20
host=jimmy
service=syslogd 1.4.1
msg=restart.
```

Par exemple, la valeur `10:03:20` correspond au troisième élément entre parenthèses de l'expression régulière dans l'événement syslog ; elle est affectée à l'attribut time *$3*. De la même manière, la valeur `jimmy` correspond au quatrième élément entre parenthèses de l'expression régulière ; elle est affectée à l'attribut host *$4*.

Constante de type chaîne

La constante de type chaîne déclare que la valeur de l'attribut est la chaîne spécifiée. Si la valeur d'attribut est une constante unique sans espace, vous devez la spécifier sans guillemets doubles (" ") comme indiqué dans l'exemple suivant :

```
severity WARNING
```

Si la valeur d'attribut comporte des espaces, vous devez par contre utiliser des guillemets doubles comme indiqué dans l'exemple suivant :

```
component "Web Server"
```

Instruction PRINTF

L'instruction PRINTF crée des valeurs d'attribut plus complexes à partir d'autres valeurs d'attribut. Elle se compose du mot clé **PRINTF** suivi d'une chaîne de format printf() de type C, ainsi que d'un ou de plusieurs noms d'attribut.

La chaîne de format ne prend en charge que l'indicateur de composant `%s`. Les valeurs des attributs utilisés dans l'instruction PRINTF doivent être dérivées à partir d'une spécification de valeur *$i* ou d'une spécification de valeur de chaîne constante (vous ne pouvez pas les déduire à partir d'une autre instruction PRINTF).

Utilisez la valeur des attributs d'argument pour composer une nouvelle chaîne constante en fonction de la chaîne de format. Cette nouvelle chaîne constante devient la valeur de l'attribut.

Dans l'exemple précédent où vous avez défini la classe de base `REGenericSyslog`, ainsi que les attributs *service* et *msg*, vous pouvez définir un attribut appelé *syslog_msg* à l'aide du mot clé **PRINTF**.

```
syslog_msg PRINTF("service %s reports %s", service, msg)
```

Si le journal consigne le message suivant :

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

Le système génère une nouvelle chaîne constante, qui comporte les valeurs d'attribut provenant de la chaîne de format :

```
syslog_msg="service syslogd 1.4.1 reports restart."
```

Mots clé :

Utilisez les mots clés dans le fichier de format pour affecter des valeurs qui se développent au moment de l'exécution.

Les mots clés suivants se développent au moment de l'exécution :

- DEFAULT
- FILENAME
- LABEL
- REGEX

DEFAULT

Le mot clé **DEFAULT** permet d'affecter une valeur DEFAULT à un attribut spécifique. L'agent de système d'exploitation affecte une valeur par défaut interne à des attributs décrits dans le tableau suivant :

Tableau 153. Attributs et valeur DEFAULT

Attributs	Description
hostname	Nom d'hôte abrégé du système sur lequel s'exécute l'agent. Il n'inclut pas le nom de domaine du système.
origin	Adresse IP du système sur lequel s'exécute l'agent.
fqhostname	Nom d'hôte complet du système sur lequel s'exécute l'agent. Il inclut le nom de domaine du système.
RemoteHost	Lorsqu'un événement apparaît sur le système local, cet attribut est vide. Si un événement se produit sur un système distant, *RemoteHost* contient une chaîne sous la forme *utilisateur@hôte:port*, qui indique le nom de l'hôte distant d'où provient l'événement, ainsi que l'utilisateur et le port utilisés pour la connexion sur cet hôte.

La valeur affectée à l'attribut *fqhostname* est influencée par les paramètres FQDomain (facultatifs) suivants dans le fichier `.conf` :

- Si vous associez FQDomain à `yes`, l'agent détermine le nom de domaine du système.
- Si vous associez FQDomain à `no` ou que vous ne lui affectez pas de valeur, l'agent ne définit pas de nom de domaine et une chaîne vide est affectée à l'attribut *fqhostname*.
- Si FQDomain n'a pas pour valeur `yes` ou `no`, le système accepte le nom de domaine comme valeur et l'ajoute au nom d'hôte.

Dans l'exemple suivant, la définition de format contient trois attributs :

- *hostname* DEFAULT
- *origin* DEFAULT
- *fqhostname* DEFAULT

Si vous associez l'attribut `FQDomain` à `yes` dans le fichier `.conf` et que vous l'exécutez sur un ordinateur avec les propriétés suivantes :

- *hostname*: `myhost`
- *IP address*: `192.168.1.100`
- *domainname*: `mycompany.com`

un événement est créé et les trois attributs prennent les valeurs suivantes :

```
"hostname=myhost", "origin=192.168.1.100", "fqhostname=myhost.mycompany.com"
```

FILENAME

Le mot clé **FILENAME** indique le nom complet (chemin inclus) du fichier journal contenant le message. Si vous utilisez un seul agent pour surveiller plusieurs fichiers journaux et que vous devez identifier la source de l'événement, utilisez ce mot clé pour compléter un attribut d'événement avec le nom de fichier. Si le message provient du journal système, le mappage correspond à `EventLog` pour les agents de système d'exploitation Windows et à `SysLogD` pour les agents de système d'exploitation UNIX.

Remarque : Le chemin inclut un attribut pour ce mot clé.

LABEL

Le mot clé **LABEL** spécifie le nom d'hôte du système sur lequel s'exécute l'agent.

REGEX

Le mot clé **REGEX** développe l'expression régulière qui correspondait au message et a provoqué l'événement.

Longueur maximale des messages :

Cette valeur correspond à la longueur maximale des messages que l'agent de système d'exploitation peut recevoir sans tronquer le message.

La longueur maximale des messages est différente dans Performance Management et Tivoli Netcool/OMNIbus.

Performance Management
Pour les événements envoyés à Performance Management, l'attribut `msgest` limité à 2048 octets. Les messages plus longs sont tronqués.

Tivoli Netcool/OMNIbus
Pour les événements envoyés à Netcool/OMNIbus via la sonde de Tivoli EIF, la taille totale de l'événement, y compris le nom de classe et tous les attributs et leurs valeurs, ne doivent pas dépasser 4 096 octets. Dans l'exemple d'événement EIF suivant, `;END` n'est pas comptabilisé dans la limite de 4096 octets. Tous les autres éléments sont néanmoins pris en compte, notamment les éléments de syntaxe (points-virgules, guillemets, signes égal).

```
Class;attr1=value1;attr2=value2;msg='Hello, world';END
```

Surveillance des fichiers journaux distants : Chiffrement d'un mot de passe ou d'une phrase de passe

Pour renforcer la sécurité du système, vous pouvez chiffrer les mots de passe et les phrases de passe transmis aux système distants lorsque vous utilisez la Surveillance des fichiers journaux distants.

Pourquoi et quand exécuter cette tâche

Le mot de passe et les phrases de passe chiffrés sont stockés dans le fichier de configuration (`.conf`). Pour plus d'informations sur le fichier de configuration, voir «Fichier de configuration», à la page 596.

Procédure

Exécutez la commande **itmpwdsnmp** et entrez le mot de passe ou la phrase de passe à chiffrer :

- Linux AIX La commande est exécutée à partir du répertoire d'installation de Cloud APM. Le chemin d'installation par défaut est `opt/ibm/apm/agent` et *rép_install* correspond à l'emplacement où vous avez installé l'agent.
- Windows Le chemin d'installation par défaut est `C:\IBM\APM`.

Linux Exemple d'exécution de la commande sous Linux :

```
$ export rép_install=/opt/ibm/apm/agent/bin
$ /opt/ibm/apm/agent/bin

Enter string to be encrypted:
motdepasse

Confirm string:
motdepasse

{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==
$
```

Dans cet exemple, le résultat de la commande, `{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==`, est utilisé dans son intégralité pour définir **SshPassword** dans le fichier de configuration de l'agent. Le préfixe `{AES256:keyfile:a}` indique à l'agent que le mot de passe est chiffré.
Pour chiffrer une phrase de passe pour un fichier de clés privées, procédez de la même manière.

Configuration de la surveillance de PHP

Vous devez configurer l'Monitoring Agent for PHP pour qu'il puisse collecter des données de l'application PHP surveillée.

Avant de commencer

1. Veillez à bien installer le package php-process. Si vous utilisez la commande `yum install` pour installer PHP, exécutez la commande `yum install php-process` pour installer le package php-process.
2. Vérifiez que le serveur HTTPD Apache est démarré avant de configurer l'agent.

   Ouvrez le fichier de configuration `httpd.conf` du serveur HTTP Apache et assurez-vous que les options `mod_status` et `ExtendedStatus On` sont activées. Par exemple :

   ```
   ExtendedStatus On
   <Location /server-status>
     SetHandler server-status
     Order deny,allow
     Allow from all
     Allow from 127.0.0.1
   </Location>
   ```

   Dans l'exemple donné, `http://127.0.0.1/server-status` doit fonctionner pour que l'agent fonctionne correctement.

   Remarque : Lynx ou Links doit être installé sous Linux pour que l'agent obtienne les données de surveillance.

   Vérifiez que la commande `apachectl status` fonctionne sur le serveur Apache surveillé sans que le code de la commande `apachectl` ne soit modifié. Lynx doit être installé pour que la commande `apachectl status` fonctionne correctement.

Pourquoi et quand exécuter cette tâche

Afin d'éviter tout problème de droits lorsque vous configurez l'agent, veillez à utiliser le même ID d'utilisateur superutilisateur ou non superutilisateur que celui utilisé pour installer l'agent. Si vous avez installé votre agent en tant qu'utilisateur sélectionné et que vous voulez le configurer en tant qu'utilisateur, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 219. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez démarrer l'agent en tant qu'un autre utilisateur, voir «Démarrage d'agents en tant qu'utilisateur non superutilisateur», à la page 1039.

L'Agent PHP est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous indiquez `PHP2` comme nom d'instance, le nom du système géré est `PHP2:hostname:PJ`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.

Procédure

- Si votre environnement est identique aux paramètres par défaut, vous pouvez utiliser le chemin d'exécution binaire par défaut, le chemin d'accès au fichier `php.ini` par défaut et le port par défaut pour configurer l'agent :
  1. Entrez :
     rép_install`/bin/php-agent.sh config` *nom_instance rép_install*`/samples/php_silent_config.txt`

Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent PHP. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

2. Pour démarrer l'agent, entrez la commande suivante :
   rép_install`/bin/php-agent.sh start` *nom_instance*

- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :
  1. Ouvrez *rép_install*`/samples/php_silent_config.txt` dans un éditeur de texte.
  2. Pour **`Location of PHP execution binary`**, vous pouvez spécifier le répertoire où se trouve l'exécution PHP. L'emplacement par défaut est `/usr/local/bin`.
  3. Pour **`Location of PHP INI file`**, vous pouvez spécifier le répertoire où se trouve le fichier `php.ini`. L'emplacement par défaut est `/etc`.
  4. Pour **`Web server port`**, vous pouvez indiquer le numéro de port du serveur Web qui exécute WordPress. La valeur par défaut est `80`.
  5. Pour **`Application DocumentRoot`**, vous pouvez spécifier le DocumentRoot de l'application PHP WordPress. Utilisez une virgule pour séparer plusieurs enregistrements. Pour permettre à l'agent de localiser tous les enregistrements d'événements, utilisez la valeur par défaut `ALL`.
  6. Sauvegardez et fermez le fichier `php_silent_config.txt`, puis entrez :
     rép_install`/bin/php-agent.sh config` *nom_instance* *rép_install*`/samples/php_silent_config.txt`
     Où *instance_name* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent PHP. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
  7. Pour démarrer l'agent, entrez la commande suivante :
     rép_install`/bin/php-agent.sh start` *nom_instance*
- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :
  1. Entrez :
     rép_install`/bin/php-agent.sh config` *nom_instance*
     Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent PHP.
  2. A l'invite `Edit Monitoring Agent for PHP settings`, entrez `1` pour continuer.
  3. A l'invite `Location of PHP execution binary`, appuyez sur Entrée pour accepter l'emplacement par défaut ou indiquez un emplacement de votre choix.
  4. A l'invite `Location of PHP INI file`, appuyez sur Entrée pour accepter l'emplacement par défaut ou indiquez un emplacement de votre choix.
  5. A l'invite `Web server port`, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez un autre numéro de port.
  6. A l'invite `Application DocumentRoot`, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez le DocumentRoot de l'application PHP WordPress. Vous pouvez utiliser une virgule pour séparer plusieurs enregistrements.
  7. Pour démarrer l'agent, entrez la commande suivante :
     rép_install`/bin/php-agent.sh start` *nom_instance*

Résultats

L'agent évalue uniquement les performances des requêtes PHP dans les applications WordPress. Le chargement CSS et JS n'est pas évalué. L'agent n'utilise pas les arguments d'URL pour identifier les URL.

Que faire ensuite

Vous pouvez vérifier que les données de l'Agent PHP s'affichent dans la console Cloud APM.

Vous devez vous assurer que le plug-in WordPress de l'agent est activé. Pour assurer l'activation, procédez comme suit :

1. Dans un navigateur Web, entrez l'URL `http://hostname:port/wp-admin/`.
2. Accédez à la page d'administration en sélectionnant **Plugins** > **Installed Plugins**.
3. Vérifiez que le plug-in Agent PHP est activé. Le plug-in de l'Agent PHP est répertorié en tant qu'**agent WordPress**. En général, le plug-in est déjà activé. Si ce n'est pas le cas, cliquez sur **Activate**.

Configuration de la surveillance PostgreSQL

Vous devez configurer l'Monitoring Agent for PostgreSQL pour qu'il puisse collecter des données de la base de données PostgreSQL surveillée.

Avant de commencer

Vous devez installer le pilote JDBC PostgreSQL avant d'installer cet agent. Le chemin d'accès à ce pilote est requis lors de la configuration de l'agent.

Le pilote JDBC de type 4 est la nouvelle version et est donc recommandé. L'utilisateur peut installer le sous-type de JDBC version 4 en fonction de la version JDK utilisée par l'agent. Pour plus d'informations sur le mappage de la version JDBC vers la version JDK, accédez au site https://jdbc.postgresql.org/download.html.

Quelques-uns des attributs collectés par l'agent s'appuient sur l'extension `pg_stat_statements`. Pour ajouter `pg_stat_statements`, installez au préalable le package `postgresql-contrib`. Vous devez modifier le fichier de configuration `postgresql.conf` pour que le serveur PostgreSQL puisse charger l'extension `pg_stat_statements`.

1. Ouvrez le fichier `postgresql.conf` dans un éditeur de texte et mettez à jour la ligne `shared_preload_libraries` :

   ```
   shared_preload_libraries = 'pg_stat_statements'
   pg_stat_statements.track_utility = false
   ```

   Ces modifications sont requises pour surveiller les instructions SQL, à l'exception des commandes d'utilitaire.

   Remarque : Le statut de `pg_stat_statements.track_utility` est défini ou modifié uniquement par un superutilisateur.
2. Redémarrez le serveur PostgreSQL après avoir mis à jour et sauvegardé le fichier `postgresql.conf`.
3. Exécutez la commande SQL suivante en utilisant psql, qui doit être connecté à la base de données qui sera fournie ultérieurement dans la configuration de l'agent pour la connectivité JDBC :

   ```
   create extension pg_stat_statements;
   select pg_stat_statements_reset();
   ```

   Remarque : La commande `create extension` et la fonction `pg_stat_statements_reset()` ne sont exécutées que par un superutilisateur.
   La vue `pg_stat_statements` doit être activée pour une base de données spécifique. Pour plus de détails, voir https://www.postgresql.org/docs/9.6/static/pgstatstatements.html.

Le fichier `pg_hba.conf` est le fichier de base de données PostgreSQL, qui contient les paramètres d'authentification. Lorsque le paramètre `auth-method` est défini sur `ident` dans le fichier `pg_hba.conf`, l'Agent PostgreSQL ne peut pas se connecter à la base de données PostgreSQL. Vérifiez que les paramètres d'authentification pour le paramètre `auth-method` sont corrects. Par exemple, vous pouvez définir les valeurs suivantes pour le paramètre `auth-method` : `md5`, `trust` ou `password`.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent PostgreSQL.

Pourquoi et quand exécuter cette tâche

L'Agent PostgreSQL est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous indiquez `PostgreSQL2` comme nom d'instance, le nom du système géré est `PostgreSQL2:hostname:PN`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 154. Versions d'agent et documentation

Version de l'Agent PostgreSQL	Documentation
01.00.13.00, 01.00.12.00, 01.00.11.00	IBM Cloud Application Performance Management
01.00.10.00	IBM Performance Management 8.1.3 *
01.00.09.00	IBM Performance Management 8.1.2*

* Le lien ouvre une rubrique Knowledge Center sur site.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour PostgreSQL**, puis cliquez sur **Configuration de l'agent**.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre Agent de surveillance pour PostgreSQL, procédez comme suit :
   a. Dans la zone **Adresse IP**, entrez l'adresse IP d'un serveur PostgreSQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.

      Remarque :

      Pour la surveillance à distance, les données des widgets **Pourcentage actuel utilisé de l'unité centrale** et **Mémoire physique utilisée (Mo)** ne sont pas disponibles sur le tableau de bord. Ces widgets affichent **N/A**.
   b. Dans la zone **Nom de base de données JDBC**, indiquez un nom de base de données pour remplacer le nom de base de données par défaut `postgres`.

c. Dans la zone **Nom d'utilisateur JDBC**, indiquez un nom d'utilisateur pour remplacer le nom d'utilisateur par défaut `postgres`.
d. Dans la zone **Mot de passe JDBC**, entrez le mot de passe de l'utilisateur JDBC.
e. Dans la zone **Confirmer le mot de passe JDBC**, entrez de nouveau le mot de passe.
f. Dans la zone **Numéro de port JDBC**, indiquez un numéro de port pour remplacer le numéro de port par défaut `5432`.
g. Dans la zone **Fichier JAR JDBC**, indiquez le chemin d'accès au connecteur PostgreSQL pour le fichier JAR Java et cliquez sur **Suivant**.
h. Dans la zone **Niveau de trace Java**, entrez le niveau de trace selon les instructions du support IBM. Le niveau de trace par défaut est `Erreur`.
i. Cliquez sur **OK**. L'instance de l'agent est affichée dans la fenêtre IBM Performance Management.

5. Cliquez avec le bouton droit de la souris sur l'instance **Agent de surveillance pour PostgreSQL**, puis cliquez sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur les systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Sur la ligne de commande, entrez la commande suivante :
   rép_install/bin/postgresql-agent.sh config *nom_instance*
2. A l'invite d'édition des paramètres PostgreSQL, entrez 1 pour continuer.
3. A l'invite d'entrée d'une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez une autre valeur et appuyez sur Entrée :
   - Adresse IP

     Remarque :

     Entrez l'adresse IP d'un serveur PostgreSQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.

     Pour la surveillance à distance, les données des widgets **Pourcentage actuel utilisé de l'unité centrale** et **Mémoire physique utilisée (Mo)** ne sont pas disponibles sur le tableau de bord. Ces widgets affichent **N/A**.
   - Nom de base de données JDBC
   - Nom d'utilisateur JDBC
   - Mot de passe JDBC
   - Numéro de port JDBC
   - Fichier JAR JDBC

   Important : La version du fichier JAR JDBC doit être identique à la version de la base de données PostgreSQL surveillée.

4. A l'invite d'entrée d'une valeur pour le paramètre `Niveau de trace Java`, entrez `2` pour accepter la valeur par défaut ou indiquez un niveau de trace selon les instructions du support IBM.
5. Exécutez la commande suivante pour démarrer l'agent :
   rép_install`/bin/postgresql-agent.sh start` *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent PostgreSQL sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans répondre aux invites, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*`/samples/postgresql_silent_config.txt`, où *rép_install* est le répertoire d'installation de l'Agent PostgreSQL. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
2. Pour éditer le fichier de configuration en mode silencieux, procédez comme suit :
   a. Pour le paramètre **`Adresse IP`**, spécifiez l'adresse IP d'un serveur PostgreSQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.

      Remarque :

      Pour la surveillance à distance, les données des widgets **Pourcentage actuel utilisé de l'unité centrale** et **Mémoire physique utilisée (Mo)** ne sont pas disponibles sur le tableau de bord. Ces widgets affichent **N/A**.
   b. Pour le paramètre **`Nom de base de données JDBC`**, indiquez un nom de base de données pour remplacer le nom de base de données par défaut `postgres`.
   c. Pour le paramètre **`Nom d'utilisateur JDBC`**, indiquez un nom d'utilisateur pour remplacer le nom par défaut `postgres`.
   d. Pour le paramètre **`Mot de passe JDBC`**, entrez le mot de passe de l'utilisateur JDBC.
   e. Pour le paramètre **`Numéro de port JDBC`**, indiquez un numéro de port pour remplacer le numéro de port par défaut `5432`.
   f. Pour le paramètre **`Fichier JAR JDBC`**, indiquez le chemin d'accès au connecteur PostgreSQL pour le fichier JAR Java si le chemin d'accès par défaut est incorrect. Le chemin d'accès par défaut du fichier JAR Java est :

```
/opt/PostgreSQL/lib/postgresql-9.3-1100.jdbc4.jar
```

Important : La version du fichier JAR JDBC doit être compatible avec la version de la base de données PostgreSQL surveillée.

g. Pour le paramètre **Niveau de trace Java**, indiquez le niveau de trace selon les instructions du support IBM. Le niveau de trace par défaut est Erreur.

3. Sauvegardez et fermez le fichier de réponses silencieux, puis exécutez la commande suivante :

```
rép_install/bin/postgresql-agent.sh config
nom_instance
rép_install/samples/postgresql_silent_config.txt
```

Où *nom_instance* est le nom à attribuer à l'instance.

4. Pour démarrer l'agent, entrez la commande suivante :

```
rép_install/bin/postgresql-agent.sh start nom_instance
```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de la surveillance Python

Les applications Python sur site et IBM Cloud peuvent être surveillées. Effectuez les étapes de configuration correspondantes en fonction de votre type d'application.

Pourquoi et quand exécuter cette tâche

Configurez le collecteur de données Python pour surveiller vos applications Python sur site et IBM Cloud.

Procédure

- Configurez le collecteur de données pour surveiller les applications IBM Cloud.
  1. Configurez le collecteur de données Python pour collecter et envoyer des données pour les applications IBM Cloud. Pour plus d'informations, voir «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 624.
  2. Facultatif : Personnalisez les fonctions de surveillance de l'collecteur de données Python. Pour plus d'informations, voir «Personnalisation du collecteur de données Python pour les applications IBM Cloud», à la page 625.
- Configurez le collecteur de données pour surveiller les applications sur site.
  1. Configurez le collecteur de données afin qu'il collecte et envoie des données au serveur Cloud APM. Pour plus d'informations, voir «Configuration du collecteur de données Python pour les applications sur site», à la page 629.
  2. Facultatif : Personnalisez les fonctions de surveillance de l'collecteur de données Python. Pour plus d'informations, voir «Personnalisation du collecteur de données Python pour les applications sur site», à la page 630.

Configuration du collecteur de données Python pour les applications IBM Cloud

Pour collecter des informations concernant les applications Python sur IBM Cloud, vous devez configurer le collecteur de données Python.

Avant de commencer

1. Assurez-vous que les applications Python que vous voulez surveiller ont des noms uniques. Le collecteur de données Python gère deux applications différentes ayant le même nom comme une seule et même application, ce qui peut entraîner des problèmes d'affichage des données sur la console Cloud APM.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Configurez le package du collecteur de données avec les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

Pourquoi et quand exécuter cette tâche

Pour configurer le collecteur de données, déployez d'abord un serveur de modules PyPi, puis installez le collecteur de données dans une application Python Django.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `python_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
2. Extrayez le module `python_datacollector_8.1.4.0.tgz`, par exemple, en exécutant la commande suivante :

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. Recherchez le fichier `manifest.yml` du serveur de packages dans le répertoire d'extraction et définissez-y le domaine, l'hôte et le nom, comme illustré dans l'exemple suivant :

   ```
   domain: mybluemix.net
   name: pythondc
   host: pythondc
   ```

   A faire : Les valeurs *host* et *name* doivent être identiques et uniques.
4. A partir du répertoire `python_dc`, envoyez l'application `pythondc` dans IBM Cloud en exécutant la commande suivante :

   ```
   cf push
   ```

5. Dans le fichier `requirements.txt` de votre application Python, ajoutez les lignes suivantes :

   ```
   cryptography==1.9.0
   --extra-index-url https://<votre_nom_hôte_et_domaine>/python-dc-repos/simple/
   ibm_python_dc
   ```

6. Dans le fichier `settings.py` de votre application Python, ajoutez `ibm_python_dc.kpg_plugin.ResourceMiddleware` au début de la section `MIDDLEWARE_CLASSES`, par exemple :

   ```
   MIDDLEWARE_CLASSES = (
       "ibm_python_dc.kpg_plugin.ResourceMiddleware",
       "mezzanine.core.middleware.UpdateCacheMiddleware",
       'django.contrib.sessions.middleware.SessionMiddleware',
       'django.middleware.common.CommonMiddleware',
   ```

7. A partir du répertoire qui contient le fichier `manifest.yml` de votre application Python, exécutez la commande suivante :

   ```
   cf push
   ```

Conseil : Pour un fichier `manifest.yml` exemple, voir «Exemple de fichier `manifest.yml`», à la page 237.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez vérifier que les données de surveillance de votre application IBM Cloud s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Personnalisation du collecteur de données Python pour les applications IBM Cloud

Vous pouvez ajouter des variables d'environnement dans l'interface utilisateur (UI) IBM Cloud pour personnaliser la surveillance de votre application IBM Cloud. Utilisez les informations suivantes pour ajouter des variables en fonction de vos besoins.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Python

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance Python sur IBM Cloud.

Tableau 155. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Python sur IBM Cloud

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https://<*IP ou nom d'hôte du serveur*>:443 • http://<*IP ou nom d'hôte du serveur*>:80	L'URL de la passerelle de serveur sur site cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n <mot de passe du fichier de clés> | base64` pour chiffrer votre mot de passe. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	http://<*serveur HTTP hébergé*>:<*port*>/keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.

Tableau 155. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Python sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KPG_ENABLE_DEEPDIVE	Facultative	• False • True	Active ou désactive la collecte des données de diagnostic. • True : La valeur par défaut. Si vous définissez cette variable sur `True`, les données de diagnostic sont collectées. • False : Si vous définissez cette variable sur `False`, les données de diagnostic ne sont pas collectées. Si vous ne définissez pas cette variable, les données de diagnostic sont collectées.
KPG_DD_CONFIG_FILE	Facultative	Nom de fichier du fichier de configuration de surveillance des diagnostics.	Nom de fichier du fichier de configuration de surveillance des diagnostics. Le nom de fichier par défaut est `kpg_dd_config.xml`. **Remarque :** Après avoir personnalisé les paramètres dans ce fichier, vous devez le placer dans le répertoire racine de l'application. Si vous ne définissez pas cette variable, le fichier de configuration par défaut `kpg_dd_config.xml` du module de collecteur de données est utilisé.
KPG_DD_APP_PATH	Facultative	Chemin d'accès de l'application Python.	Le chemin d'accès de l'application Python ou du module pour lequel le collecteur de données collecte des données de diagnostic. Séparez les chemins d'accès des différentes applications et modules Python que vous voulez surveiller à l'aide d'un point-virgule **;**. Si vous ne définissez pas cette variable, le collecteur de données collecte des données pour les demandes et les modules que votre d'application utilise. Les données des demandes dans la lib Python ne sont pas collectées.

Tableau 155. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Python sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KPG_DD_SECURITY_FILTER	Facultative	• True • False	• True : La valeur par défaut. Si vous définissez cette variable sur `True`, les valeurs (telles que les mots de passe) sont masquées dans les instructions SQL et les paramètres ne sont pas affichés dans le widget de groupe **Contexte des demandes**. • False : Si vous définissez cette variable sur `False`, les valeurs (telles que les mots de passe) ne sont pas masquées dans les instructions SQL et les paramètres sont affichés dans le widget de groupe **Contexte des demandes**. Si vous ne définissez pas cette variable, les valeurs (telles que les mots de passe) sont masquées dans les instructions SQL et les paramètres ne sont pas affichés dans le widget de groupe **Contexte des demandes**.
KPG_GC_STATS	Facultative	True	Toutes les fonctions statistiques de récupération de place de Python sont activées. Lorsque vous définissez cette valeur sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Pour désactiver KPG_GC_STATS, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. **Remarque :** Ne définissez jamais `KPG_SAVE_ALL=True` dans votre environnement de production officiel. C'est uniquement réservé au mode débogage. Assurez-vous que la mémoire affectée à l'application est suffisante.

Tableau 155. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Python sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KPG_LOG_LEVEL	Facultative	• DEBUG • ERROR • INFO	• DEBUG : Seules les informations de débogage utiles sont imprimées dans le journal, par exemple, les données collectées, les données envoyées au serveur et la réponse du serveur. • ERROR : Seules les informations concernant les exceptions et les situations imprévues sont imprimées dans le journal. • INFO : Les informations récapitulatives concernant le collecteur de données permettant à l'utilisateur d'être informé de ses activités sont imprimées dans le journal.
KPG_LOG_TOCONSOLE	Facultative	• Y • True • Toute autre valeur qui n'est pas `False`	Le journal est imprimé vers la console et vous pouvez l'afficher en exécutant la commande **`cf logs <nom_app>`**.
KPG_SAVE_ALL	Facultative	True	Tous les objets non référencés sont sauvegardés dans `gc.garbage`, et vous devez effacer `gc.garbage` toutes les minutes (le collecteur de données l'efface pour vous). Lorsque la valeur est définie sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.SAVE_ALL)` Pour désactiver KPG_SAVE_ALL, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. **Remarque :** Ne définissez jamais `KPG_SAVE_ALL=True` dans votre environnement de production officiel. C'est uniquement réservé au mode débogage. Assurez-vous que la mémoire affectée à l'application est suffisante.

Annulation de la configuration du collecteur de données Python pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller votre environnement Python ou si vous souhaitez mettre à niveau le collecteur de données Python, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Python.

Procédure

1. Accédez au répertoire de base de votre application Python.
2. Supprimez les lignes suivantes du fichier `requirements.txt` de l'application :

```
--extra-index-url https://<votre_nom_hôte_et_domaine>/python_dc/static/python-dc-repos/simple/
ibm-python-dc
```

3. Dans le fichier `settings.py`, supprimez la ligne suivante de la section `MIDDLEWARE_CLASSES` :

   ```
   ibm_python_dc.kpg_plugin.ResourceMiddleware
   ```

4. Exécutez la commande suivante pour renvoyer l'application afin que les modifications soient prises en compte :

   ```
   cf push
   ```

Résultats

Vous avez correctement annulé la configuration du collecteur de données Python.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Configuration du collecteur de données Python pour les applications sur site

Pour collecter des informations sur les applications Python exécutées dans votre environnement local, vous devez configurer le collecteur de données Python.

Avant de commencer

1. Assurez-vous que les applications Python que vous voulez surveiller ont des noms uniques. Le collecteur de données Python gère deux applications différentes ayant le même nom comme une seule et même application, ce qui peut entraîner des problèmes d'affichage des données sur la console Cloud APM.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Configurez le package du collecteur de données avec les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

Pourquoi et quand exécuter cette tâche

La procédure suivante configure le collecteur de données dans votre application Python avec les paramètres par défaut. Pour personnaliser la configuration du collecteur de données, utilisez des variables d'environnement dans les fichiers de configuration du collecteur de données. Pour plus d'informations, voir «Personnalisation du collecteur de données Python pour les applications sur site», à la page 630.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `python_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
2. Procédez à l'extraction des fichiers à partir du module du collecteur de données, par exemple en exécutant la commande suivante :

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. Depuis le répertoire `python_dc`, exécutez la commande suivante :

   ```
   python server.py
   ```

4. Exécutez la commande suivante :

   ```
   pip install ibm_python_dc --extra-index-url http://nom ou adresse IP de l'hôte:8000/
   python-dc-repos/simple/ --trusted-host nom ou adresse IP de l'hôte
   ```

   où *nom ou IP de l'hôte* est le nom ou l'adresse IP de l'hôte permettant d'exécuter votre référentiel de collecteur de données Python.

   Important : Utilisez le nom ou l'adresse IP pour spécifier l'hôte de l'URL et l'hôte sécurisé dans cette commande. Par exemple, si vous spécifiez l'hôte en utilisant l'adresse IP `9.42.36.180`, la commande est la suivante :

   ```
   pip install ibm_python_dc --extra-index-url http://9.42.36.180:8000/
   python-dc-repos/simple/ --trusted-host 9.42.36.180
   ```

5. Dans le fichier `settings.py` de votre application Python, ajoutez `ibm_python_dc.kpg_plugin.ResourceMiddleware` à la section `MIDDLEWARE_CLASSES` au format utilisé dans l'exemple suivant :

   ```
   MIDDLEWARE_CLASSES = (
       "ibm_python_dc.kpg_plugin.ResourceMiddleware",
       "mezzanine.core.middleware.UpdateCacheMiddleware",
       'django.contrib.sessions.middleware.SessionMiddleware',
       'django.middleware.common.CommonMiddleware',
   ```

Résultats

Le collecteur de données est configuré avec les paramètres par défaut et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez désormais vous connecter au serveur Cloud APM pour afficher les données de surveillance.

A faire : Après avoir ajouté votre application Python à la console Cloud APM, vous pouvez afficher ses données de surveillance dans le composant nommé application Python Runtime.

Pour obtenir des instructions de démarrage de la serveur Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Personnalisation du collecteur de données Python pour les applications sur site

En modifiant des fichiers dans le module de collecteur de données, vous pouvez définir les variables d'environnement de façon à personnaliser la surveillance pour votre application Python.

Deux fichiers sont fournis pour personnaliser les paramètres du collecteur de données, `global.environment` et `config.properties`. Après avoir modifié les paramètres dans ces fichiers, redémarrez l'application Python pour que les modifications soient prises en compte.

En modifiant le fichier `global.environment`, vous pouvez personnaliser la connexion entre le collecteur de données et le serveur Cloud APM. Si vous voulez utiliser un autre serveur Cloud APM au lieu de la valeur par défaut, ou si le fichier de clés ou son mot de passe est changé, modifiez le serveur Cloud APM de façon à reconnecter le collecteur de données au serveur Cloud APM.

En modifiant le fichier `config.properties`, vous pouvez personnaliser le comportement du collecteur de données en fonction de vos besoins, par exemple, activer ou désactiver la trace de méthode.

Le fichier de configuration `global.environment`

Le tableau 156 indique les variables d'environnement que vous pouvez définir dans le fichier de configuration `global.environment`, ainsi que leur description. Vous pouvez trouver le fichier `global.environment` dans le dossier `etc` dans lequel votre collecteur de données Python est installé, par exemple, dans le répertoire `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc/etc`.

Tableau 156. Variables d'environnement prises en charge dans le fichier `global.environment`

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https: *//<IP ou nom d'hôte du serveur>*: 443 • http: *//<IP ou nom d'hôte du serveur>*:80	L'URL de la passerelle de serveur sur site cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe du fichier de clés	Le mot de passe du fichier de clés qui est apparié avec le fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	http://*<serveur http hébergé>*:*<port>*/ keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.

Le fichier `config.properties`

Le tableau 157 indique les variables d'environnement que vous pouvez définir dans le fichier de configuration `config.properties`, ainsi que leur description. Vous pouvez trouver le fichier `config.properties` dans le répertoire d'installation de votre collecteur de données Python, par exemple, dans le répertoire `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc`.

Tableau 157. Variables d'environnement prises en charge dans le fichier `config.properties`

Nom de la variable	Importance	Valeur	Description
KPG_ENABLE_DEEPDIVE	Facultative	• False • True	• False : La valeur par défaut. Si vous définissez cette variable sur `False`, les données de diagnostic ne seront pas collectées. • True : Si vous définissez cette variable sur `True`, les données de diagnostic seront collectées. La valeur par défaut est `True`. Si vous ne définissez pas cette variable, les données de diagnostic ne seront pas collectées.

Tableau 157. Variables d'environnement prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KPG_DD_CONFIG_FILE	Facultative	Nom de fichier du fichier de configuration de surveillance des diagnostics.	Nom de fichier du fichier de configuration de surveillance des diagnostics. Le nom de fichier par défaut est `kpg_dd_config.xml`. **Remarque :** Après avoir personnalisé les paramètres dans ce fichier, vous devez le placer dans le répertoire racine de l'application. Si vous ne définissez pas cette variable, le fichier de configuration par défaut `kpg_dd_config.xml` du module de collecteur de données sera utilisé.
KPG_DD_APP_PATH	Facultative	Chemin d'accès de l'application Python.	Le chemin d'accès de l'application Python ou du module pour lequel le collecteur de données collecte des données de diagnostic. Séparez les chemins d'accès des différentes applications et modules Python que vous voulez surveiller à l'aide d'un point-virgule `;`. Si vous ne définissez pas cette variable, le collecteur de données collectera des données pour les demandes et les modules que votre d'application utilise. Les données des demandes dans la lib Python ne seront pas collectées.
KPG_DD_SECURITY_FILTER	Facultative	• True • False	• True : La valeur par défaut. Si vous définissez cette variable sur `True`, les valeurs (telles que les mots de passe) seront masquées dans les instructions SQL et les paramètres ne seront pas affichés dans le widget de groupe **Contexte des demandes**. • False : Si vous définissez cette variable sur `False`, les valeurs (telles que les mots de passe) ne seront pas masquées dans les instructions SQL et les paramètres ne seront pas affichés dans le widget de groupe **Contexte des demandes**. Si vous ne définissez pas cette variable, les valeurs (telles que les mots de passe) seront masquées dans les instructions SQL et les paramètres ne seront pas affichés dans le widget de groupe **Contexte des demandes**.

Tableau 157. Variables d'environnement prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KPG_GC_STATS	Facultative	True	Toutes les fonctions statistiques de récupération de place de Python sont activées. Lorsque vous définissez cette valeur sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Pour désactiver KPG_GC_STATS, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. La valeur par défaut est `True`. **Remarque :** Ne définissez jamais `KPG_GC_STATS=True` dans votre environnement de produit officiel. C'est uniquement réservé au mode débogage. Et assurez-vous que la mémoire affectée à l'application est suffisante.
KPG_LOG_LEVEL	Facultative	• DEBUG • ERROR • INFO	• DEBUG : Seules les informations de débogage utiles seront imprimées dans le journal, par exemple, les données collectées, les données envoyées au serveur et la réponse du serveur. • ERROR : Seules les informations concernant les exceptions et les situations très imprévues seront imprimées dans le journal. • INFO : Les informations récapitulatives concernant le collecteur de données permettant à l'utilisateur d'être informé de ses activités seront imprimées dans le journal. La valeur par défaut est `ERROR`.
KPG_LOG_TOCONSOLE	Facultative	• Y • True • Toute autre valeur qui n'est pas `False`	Le journal sera imprimé vers la console et vous pourrez l'afficher en exécutant la commande **`cf logs <nom_app>`**. La valeur par défaut est `True`.

Tableau 157. Variables d'environnement prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KPG_SAVE_ALL	Facultative	True	Tous les objets non référencés seront sauvegardés dans `gc.garbage`, et vous devrez effacer `gc.garbage` toutes les minutes (le collecteur de données l'effacera pour vous). Lorsque la valeur est définie sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.SAVE_ALL)` Pour désactiver KPG_SAVE_ALL, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. La valeur par défaut est `True`. **Remarque :** Ne définissez jamais `KPG_SAVE_ALL=True` dans votre environnement de produit officiel. C'est uniquement réservé au mode débogage. Et assurez-vous que la mémoire affectée à l'application est suffisante.
APM_GW_PROXY_CONNECTION	Facultative	http://*<IP ou nom d'hôte du serveur>*:port	Le proxy HTTP ou HTTPS que le collecteur de données Python utilise pour envoyer des données de surveillance.

Annulation de la configuration du collecteur de données Python pour les applications sur site

Si vous n'avez pas besoin de surveiller votre environnement Python ou si vous souhaitez mettre à niveau le collecteur de données Python, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Python.

Procédure

1. Accédez au répertoire de base de votre application Python.
2. Supprimez les lignes suivantes du fichier `requirements.txt` de l'application :
   ```
   --extra-index-url https://<votre_nom_hôte_et_domaine>/python_dc/static/python-dc-repos/simple/
   ibm-python-dc
   ```
3. Dans le fichier `settings.py`, supprimez la ligne suivante de la section `MIDDLEWARE_CLASSES` :
   ```
   ibm_python_dc.kpg_plugin.ResourceMiddleware
   ```
4. Exécutez la commande `pip uninstall ibm_python_dc` pour désinstaller le collecteur de données Python de l'exécution Python.

Résultats

Vous avez correctement annulé la configuration du collecteur de données Python.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Configuration de la surveillance de RabbitMQ

L'Monitoring Agent for RabbitMQ surveille l'état de santé et les performances des ressources du cluster RabbitMQ, telles que les noeuds, les files d'attente et les canaux du cluster. Vous devez configurer l'agent RabbitMQ afin qu'il puisse collecter des données RabbitMQ.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel.
- Assurez-vous que l'utilisateur de RabbitMQ qui se connecte au noeud dispose du droit de lecture et que la balise de surveillance, d'administrateur ou de gestion est activée pour cet utilisateur.
- Assurez-vous que le plug-in de gestion de RabbitMQ est activé sur tous les noeuds du cluster, parce qu'en cas d'échec d'un noeud du cluster, l'agent RabbitMQ se connecte à un noeud homologue qui est disponible dans le cluster.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent RabbitMQ.

Pourquoi et quand exécuter cette tâche

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir agent RabbitMQ. Pour accéder à la documentation de la version 1.0.0, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management.

L'agent RabbitMQ est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Pour pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour RabbitMQ**, puis cliquez sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la zone **Entrez un nom d'instance unique**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre Agent de surveillance pour RabbitMQ, indiquez des valeurs pour les paramètres de configuration et cliquez sur **Suivant**.

   Pour plus d'informations sur les paramètres de configuration, voir la rubrique suivante : «Paramètres de configuration de l'agent», à la page 637
5. Cliquez avec le bouton droit de la souris sur l'instance **Agent de surveillance pour RabbitMQ**, puis cliquez sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur les systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, entrez la commande suivante : *rép_install*/bin/rabbitmq.sh config *nom_instance* où *nom_instance* est le nom que vous voulez donner à l'instance :
2. Lorsque vous êtes invité à saisir une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une valeur et appuyez sur Entrée :
   - Adresse IP
   - Nom d'utilisateur
   - Mot de passe
   - Numéro de port
   - Accueil Java
   - Niveau de trace Java

   Pour plus d'informations sur les paramètres de configuration, voir la rubrique suivante : «Paramètres de configuration de l'agent», à la page 637
3. Exécutez la commande suivante pour démarrer l'agent :
   rép_install/bin/rabbitmq.sh start *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent RabbitMQ sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*\samples\rabbitmq_silent_config.txt
2. Dans le fichier rabbitmq_silent_config.txt, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour plus d'informations sur les paramètres de configuration, voir la rubrique suivante : «Paramètres de configuration de l'agent»
3. Sauvegardez le fichier de réponses, puis exécutez la commande suivante :

   Linux AIX *rép_install*/bin/rabbitmq-agent.sh config *rép_install*/samples/rabbitmq_silent_config.txt

   Windows *rép_install*/bin/rabbitmq-agent.bat config *rép_install*/samples/rabbitmq_silent_config.txt
4. Démarrez l'agent :

   Linux AIX Exécutez la commande suivante : *rép_install*\bin\rabbitmq-agent.sh start

   Windows Cliquez avec le bouton droit de la souris sur **Agent de surveillance pour RabbitMQ**, puis cliquez sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'agent RabbitMQ, vous pouvez modifier les valeurs par défaut des paramètres, comme le nom de l'instance et les certificats de validation SSL.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'agent RabbitMQ.

Tableau 158. Noms et descriptions des paramètres de configuration pour l'agent RabbitMQ

Nom de paramètre	Description	Zone obligatoire
Adresse IP	Adresse IP du noeud sur lequel l'application RabbitMQ est installée.	Oui
Nom d'utilisateur	Nom de l'utilisateur RabbitMQ.	Yes
mot de passe	Mot de passe permettant de se connecter à l'interface utilisateur de gestion RabbitMQ.	Yes
Confirmer le mot de passe	Mot de passe que vous avez entré dans la zone **Password**.	Yes
Numéro de port	Numéro de port où le plug-in de gestion RabbitMQ est activé. Utilisez le numéro de port par défaut 15672 ou spécifiez un autre numéro de port.	Non
Répertoire de base Java	Chemin où le plug-in Java est installé. Utilisez le chemin d'accès par défaut C:\Program Files\IBM\Java50 ou le répertoire où est installé le plug-in Java.	Non

Tableau 158. Noms et descriptions des paramètres de configuration pour l'agent RabbitMQ (suite)

Nom de paramètre	Description	Zone obligatoire
Niveau de trace Java	Niveau de trace du fournisseur Java. Les valeurs de niveau de trace valides sont les suivantes : • OFF • ERROR • WARN • INFO • DEBUG_MAX • ALL	Non

Configuration de la surveillance des temps de réponse

L'agent Response Time Monitoring surveille les transactions HTTP et HTTPS sur votre serveur HTTP. Les transactions réelles des utilisateurs sur le navigateur (temps du navigateur) sont également surveillées.

L'agent Response Time Monitoring peut être utilisé pour visualiser les niveaux suivants d'informations de surveillance :

Surveillance des transactions HTTP et HTTPS

La surveillance des transactions HTTP est automatiquement disponible lorsque vous installez l'agent Response Time Monitoring.

Selon le type de serveur HTTP que vous surveillez, la surveillance des transactions HTTPS peut être disponible automatiquement ou elle peut nécessiter une configuration manuelle. Pour plus d'informations, voir «Response Time Monitoring Composants», à la page 639.

L'agent Response Time Monitoring surveille également les données relatives aux nombres d'utilisateurs, aux nombres de sessions et aux périphériques.

Les données sont présentées sur le tableau de bord Transactions utilisateur final à l'heure locale de l'utilisateur, et elles sont également utilisées dans le widget Demandes et temps de réponse.

Surveillance des transactions réelles des utilisateurs (temps du navigateur)

Selon le type de serveur HTTP que vous surveillez, les temps du navigateur peuvent être disponibles automatiquement ou il peut être nécessaire de les configurer. Pour plus d'informations, voir «Response Time Monitoring Composants», à la page 639.

Les temps du navigateur sont rendus possibles grâce à JavaScript Injection.

JavaScript Injection vous permet d'afficher davantage de widgets et de détails dans les tableaux de bord Transactions utilisateur final. JavaScript Injection veille à ce que le temps de réponse réel de l'utilisateur final soit collecté à partir du navigateur. Il surveille les performances des pages HTTP et des objets imbriqués pour les pages Web servies par le serveur HTTP. Les détails supplémentaires suivants relatifs aux transactions réelles des utilisateurs finaux sont disponibles :

- Le Temps total client dans le widget Demandes et temps de réponse des transactions
- Le Temps de réponse pour les transactions Temps client dans le widget Transactions - 10 premières
- Répartition des temps de rendu

Pour plus d'informations sur la façon de configurer JavaScript injection, voir «Injection JavaScript», à la page 642

Affichage des tableaux de bord de transactions

Affichez les données de transaction dans le Tableau de bord d'Application Performance.

Un certain nombre de widgets sont disponibles dans le Tableau de bord d'Application Performance et fournissent des détails contextuels sur les transactions.

Les *demandes correctes* ont un temps de réponse inférieur à 10 secondes. Les *demandes lentes* ont un temps de réponse supérieur à 10 secondes. La valeur de 10 secondes utilisée pour déterminer si le temps de réponse est correct ou lent n'est pas configurable. Les widgets suivants sont disponibles :

- Widget de groupe Les pires utilisateurs - 5 premiers
- Widget de groupe Les pires appareils - 5 premiers
- Widget de groupe Demandes et temps de réponse
- Widget de groupe Transactions - 10 premières
- Widget de groupe Demandes et temps de réponse des transactions
- Widget de groupe S'exécute sur
- Widget de groupe Sous-transactions
- Widget de groupe Instances de transaction
- Widget de groupe Utilisateurs par emplacement
- Widget de groupe Utilisateurs à l'emplacement sélectionné
- Widget de groupe Sessions utilisateur à l'emplacement sélectionné - 10 premières
- Widget de groupe Demandes et temps de réponse d'utilisateur
- Widget de groupe Sessions utilisateur - 10 premières
- Widget de groupe Demandes et temps de réponse d'unité
- Widget de groupe Session
- Widget de groupe Demandes de session
- Widget de groupe Instances de session
- Widget de groupe Instances de transaction
- Tableau de bord Récapitulatif des transactions de middleware
- Tableau de bord Détails des transactions de middleware

  Remarque : Par défaut, ce tableau de bord affiche les détails de l'instance concernant les 4 dernières heures uniquement. Si vous souhaitez afficher les détails d'instance des transactions de middleware sur une durée plus longue, vous devez configurer le serveur Cloud APM pour qu'il conserve ces données pendant plus de 4 heures. Pour plus d'informations, voir «Conservation des transactions de middleware», à la page 1100.
- Seuils d'événement pour la surveillance des transactions
- Données d'agrégation d'interaction
- Données d'agrégation de transactions
- Statut de la transaction WRT

Response Time Monitoring Composants

Les fonctionnalités de base de l'agent Response Time Monitoring sont les suivantes :

- surveillance des transactions HTTP
- surveillance des transactions HTTPS
- Surveillance des temps du navigateur (à l'aide de JavaScript Injection)

Pour voir des descriptions plus détaillées de ces fonctionnalités, voir «Configuration de la surveillance des temps de réponse», à la page 638.

Selon le type de serveur HTTP que vous surveillez, la fonctionnalité de base de l'agent Response Time Monitoring est assurée par l'utilisation de l'un des composants suivants :

- module IBM HTTP Server Response Time
- Analyseur de paquets

Si vous surveillez un serveur IBM HTTP Server ou Apache HTTP Server, il est recommandé d'utiliser le module IBM HTTP Server Response Time. Il est possible, mais déconseillé, d'utiliser Analyseur de paquets.

Si vous surveillez Sun Java System Web Server ou Microsoft Internet Information Services, utilisez Analyseur de paquets. Le module IBM HTTP Server Response Time n'est pas pris en charge sur Sun Java System Web Server ou Microsoft Internet Information Services. Analyseur de paquets est pris en charge sous Windows, Linux et AIX.

Planification de l'installation

Planifiez votre installation de l'agent Response Time Monitoring en fonction de votre système d'exploitation et du type de serveur HTTP.

La fonctionnalité de base de l'agent Response Time Monitoring peut être assurée par l'utilisation de l'un des composants suivants :

- Analyseur de paquets
- module IBM HTTP Server Response Time

Vous déterminez quel composant utiliser en fonction des considérations suivantes :

- Le type de serveur HTTP sur lequel vous installez l'agent Response Time Monitoring.
- Le système d'exploitation sur lequel le serveur HTTP est installé.

Les éléments à prendre en considération lors de l'installation de l'agent Response Time Monitoring avec Analyseur de paquets sont les suivants :

- Analyseur de paquets est pris en charge sur tous les systèmes d'exploitation (Windows, Linux et AIX).
- Analyseur de paquets surveille les transactions HTTP sur le port 80 pour tous les systèmes d'exploitation.
- La surveillance des transaction HTTPS n'est pas automatique et doit être configurée manuellement. L'agent Response Time Monitoring a besoin d'accéder aux certificats SSL pour pouvoir déchiffrer le trafic SSL provenant des serveurs HTTP. Pour plus d'informations, voir «Surveillance des transactions HTTPS», à la page 658.
- Analyseur de paquets est pris en charge sur tous les serveurs HTTP, mais il est seulement recommandé pour Sun Java System Web Server et Microsoft Internet Information Services.
- AIX Linux Windows Pour installer l'agent Response Time Monitoring pour qu'il fonctionne avec Analyseur de paquets sur un serveur IBM HTTP ou Apache HTTP, le serveur HTTP doit être arrêté. Lorsque vous installez l'agent Response Time Monitoring et que le serveur HTTP est arrêté, Analyseur de paquets est automatiquement activé.
- AIX Linux Windows Bien que Analyseur de paquets puisse être configuré pour un serveur IBM HTTP Server ou Apache HTTP Server, il n'est pas recommandé ; le module IBM HTTP Server Response Time est recommandé.
- Windows WinPcap 4.1.3 est requis préalablement à l'installation de l'agent Response Time Monitoring.
- Windows AIX Linux Si vous installez l'agent Response Time Monitoring sur Sun Java System Web Server ou Microsoft Internet Information Services, Analyseur de paquets est configuré automatiquement.

Les éléments à prendre en considération pour l'installation de l'agent Response Time Monitoring avec le module IBM HTTP Server Response Time sont les suivants :

- module IBM HTTP Server Response Time est pris en charge sur tous les systèmes d'exploitation (Windows, Linux et AIX). Le module IBM HTTP Server Response Time prend en charge IBM HTTP Server version 7, 8 et 9.
- Le module IBM HTTP Server Response Time surveille les demandes HTTP et HTTPS sur tous les ports sous AIX, Linux et Windows.
- Le module IBM HTTP Server Response Time est seulement pris en charge pour IBM HTTP Server ou Apache HTTP Server.
- Le module IBM HTTP Server Response Time est un composant de l'agent HTTP Server. Vous devez installer l'agent HTTP Server soit avant l'agent Response Time Monitoring, soit en même temps. Pour plus d'informations, voir «module IBM HTTP Server Response Time», à la page 648.
- Les deux agents démarrent automatiquement, mais vous devez redémarrer le serveur HTTP.

Le tableau suivant décrit les différentes combinaisons pour configurer automatiquement l'agent Response Time Monitoring.

Tableau 159. Scénarios pour la configuration automatique de l'agent Response Time Monitoring

Combinaisons de serveur HTTP et de système d'exploitation	**Analyseur de paquets**	**module IBM HTTP Server Response Time**
Sun Java System Web Server ou Microsoft Internet Information Services sous AIX ou Linux	Automatique	Non pris en charge
Sun Java System Web Server ou Microsoft Internet Information Services sous Windows	Automatique	Non pris en charge
IBM HTTP Server ou Apache HTTP Server sous AIX, Linux ou Windows	Automatique si le serveur HTTP est arrêté.	Automatique si le serveur HTTP est présent et configuré

Planification de la configuration

La surveillance HTTP est activée automatiquement lorsque vous installez l'agent Response Time Monitoring. Selon votre environnement, il peut être nécessaire de configurer HTTPS et JavaScript Injection manuellement.

Surveillance du protocole HTTP
La surveillance des transactions HTTP est configurée automatiquement pour Analyseur de paquets et pour le module IBM HTTP Server Response Time, si vous suivez les instructions d'installation. Voir «Planification de l'installation», à la page 640.

Surveillance du protocole HTTPS
La surveillance des transactions HTTPS est configurée automatiquement pour le module IBM HTTP Server Response Time si vous suivez les instructions d'installation. Voir «Planification de l'installation», à la page 640.

La surveillance des transactions HTTPS doit être configurée manuellement pour Analyseur de paquets. Pour plus d'informations, voir «Organigramme de l'Analyseur de paquets», à la page 656.

Temps du navigateur (à l'aide de JavaScript Injection)
Les temps du navigateur (à l'aide de JavaScript Injection) sont configurés automatiquement pour le module IBM HTTP Server Response Time.

Les temps du navigateur (à l'aide de JavaScript Injection) doivent être configurés manuellement pour Analyseur de paquets. Pour plus d'informations, voir «Organigramme de l'Analyseur de paquets», à la page 656.

Le tableau suivant décrit la façon dont la fonctionnalité de base est configurée pour chaque composant :

Tableau 160. Configuration de la fonctionnalité de base

	Analyseur de paquets sur Sun Java System Web Server ou Microsoft Internet Information Services (Windows, Linux ou AIX)	**module IBM HTTP Server Response Time sur IBM HTTP Server ou Apache HTTP Server (Windows, Linux ou AIX)**
Surveillance des transactions HTTP	Activée automatiquement.	Activée automatiquement
Surveillance des transactions HTTPS	Doit être configurée manuellement.	Activée automatiquement
Surveillance des transactions réelles des utilisateurs (temps du navigateur) à l'aide de JavaScript Instrumentation	Doit être configurée manuellement.	Activée automatiquement

Injection JavaScript

Vous pouvez personnaliser les données collectées par l'agent Response Time Monitoring pour l'affichage dans les tableaux de bord Transactions utilisateur final.

Pour assurer un bon acquis utilisateur pour une application Web, vous devez surveiller les performances telles qu'elles sont perçues par les utilisateurs réels. Cela implique une surveillance au niveau du navigateur.

Pour pouvoir surveiller au niveau du navigateur, vous devez injecter du code de surveillance JavaScript dans les pages que vous voulez surveiller. Ce code collecte alors des données pour des temps de navigateur spécifiques.

Cela est possible grâce à l'injection JavaScript dans les pages Web et les objets que vous souhaitez surveiller. Selon le type de serveur HTTP sur lequel vous avez installé votre agent Response Time Monitoring, il existe deux méthodes que vous pouvez utiliser pour collecter des informations sur le temps de réponse moyen des transactions pour l'utilisateur final réel.

- Si vous utilisez un serveur IBM HTTP Server ou Apache HTTP Server, utilisez le module IBM HTTP Server Response Time. Le module IBM HTTP Server Response Time effectue automatiquement l'injection JavaScript. Le module IBM HTTP Server Response Time est un composant de l'agent HTTP Server. Il est installé et configuré en tant qu'élément de l'agent HTTP Server. Pour plus d'informations, voir «module IBM HTTP Server Response Time», à la page 648.
- Si vous utilisez n'importe quel autre serveur HTTP pris en charge, utilisez Analyseur de paquets. Avec Analyseur de paquets, vous devez instrumenter manuellement vos pages Web pour la collecte des temps du navigateur. Pour plus d'informations, voir «Ajout du composant de surveillance JavaScript à votre application», à la page 657.

Le tableau suivant indique les fonctions qui sont disponibles dans le Tableau de bord d'Application Performance si vous configurez votre environnement pour Analyseur de paquets ou pour le module IBM HTTP Server Response Time :

	Analyseur de paquets	**module IBM HTTP Server Response Time**
10 premières transactions	✓	✓
Temps serveur	✓	✓
Répartition des temps de rendu	—	✓

	Analyseur de paquets	module IBM HTTP Server Response Time
Sous-transactions AJAX	✓	✓
Données de temporisation des ressources dans la table Sous-transactions	—	✓
Instances de transaction (10 premières)	✓	✓
Topologie des instances de transaction	✓	✓
Topologie des applications	✓	✓
Instrumentation automatique de l'injection de JavaScript	N/A	✓

Reconfiguration de la Response Time Monitoring sous Windows

Utilisez la commande de configuration interactive `rt-agent` ou la fenêtre IBM Cloud Application Performance Management pour configurer ou reconfigurer l'agent.

Pourquoi et quand exécuter cette tâche

L'agent de Response Time Monitoring est configuré automatiquement après l'installation. Suivez les instructions d'installation : «Planification de l'installation», à la page 640. Il se peut que vous deviez effectuer une reconfiguration, par exemple si vous voulez surveiller un port différent ou surveiller des transactions HTTPS.

Le répertoire d'installation est appelé *rép_install*. Le chemin d'accès au répertoire d'installation par défaut est : `C:\IBM\APM\`

Procédure

Pour personnaliser vos paramètres de données, procédez comme suit :

1. Sur l'ordinateur sur lequel l'agent Response Time Monitoring est installé, arrêtez l'agent :
   rép_install`\BIN\rt-agent.bat stop`
2. Utilisez la configuration silencieuse pour configurer l'agent :
   rép_install`\BIN\rt-agent.bat config` *rép_install*`\samples\rt_silent_config.txt`

   Pour activer la surveillance des transactions HTTPS : supprimez la mise en commentaire des lignes suivantes dans le fichier de configuration en mode silencieux :

   ```
   # Monitor HTTPS transactions
   KT5MONITORHTTPSAPP=Yes

   # HTTPS keystore (e.g. - /tmp/keys.kdb)
   KT5KEYSTORE=C:\keys\keys.kdb

   # HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
   KT5SERVERMAP=certalias,9.48.152.1,443
   ```
3. Redémarrez l'agent Response Time Monitoring pour que les modifications soient prises en compte :
   rép_install`\BIN\rt-agent.bat start`

Résultats

Les données de la nouvelle source sont affichées dans les tableaux de bord associés à Response Time Monitoring.

Reconfiguration de la Response Time Monitoring sur AIX et Linux

Utilisez la commande de configuration `rt-agent` pour configurer ou reconfigurer l'agent de Response Time Monitoring.

Pourquoi et quand exécuter cette tâche

L'agent de Response Time Monitoring est configuré automatiquement après l'installation. Suivez les instructions d'installation : «Planification de l'installation», à la page 640. Il se peut que vous deviez effectuer une reconfiguration,par exemple si vous voulez surveiller un port différent.

Le répertoire d'installation est appelé *rép_install*. Le répertoire d'installation par défaut est : `/opt/ibm/apm/agent`.

Utilisez le même utilisateur root que celui que vous avez utilisé pour démarrer, arrêter et configurer l'agent.

Procédure

Pour effectuer une reconfiguration, procédez comme suit :

1. Sur l'ordinateur sur lequel l'agent Response Time Monitoring est installé, arrêtez l'agent : *rép_install*`/bin/rt-agent.sh stop`
2. Utiliser une configuration en mode silencieux ou interactive :
   a. Configuration interactive :
      rép_install`/bin/rt-agent.sh config`
   b. Configuration en mode silencieux :
      rép_install`/bin/rt-agent.sh config` *rép_install*`/samples/rt_silent_config.txt`
3. Redémarrez l'agent Response Time Monitoring pour que les modifications soient prises en compte : *rép_install*`/bin/rt-agent.sh start`

Résultats

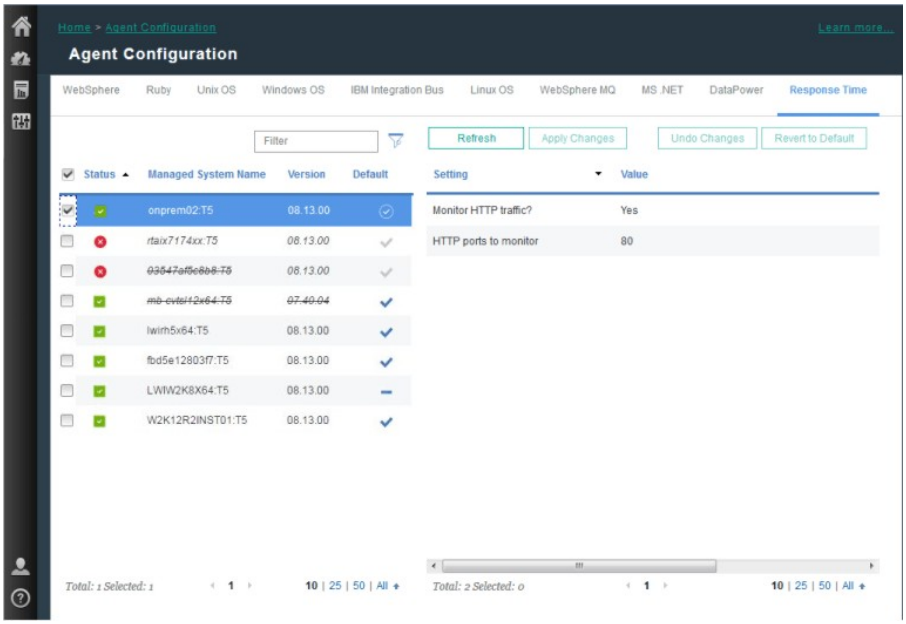
Les données de la nouvelle source sont affichées dans les tableaux de bord associés à Response Time Monitoring.

Configuration à l'aide de la page Configuration d'agent

Vous pouvez utiliser la page Configuration d'agent dans la console Cloud APM pour voir quels agents sont installés. Vous pouvez, le cas échéant, désactiver ou activer la surveillance des transactions HTTP et définir les ports surveillés par les agents Response Time Monitoring.

Configuration d'agent

Pour accéder à la page Configuration d'agent Response Time Monitoring dans la console Cloud APM, sélectionnez **Configuration du système** > **Configuration d'agent**, puis sélectionnez l'onglet **Temps de réponse**.



La page Configuration d'agent répertorie les systèmes de votre environnement sur lesquels Response Time Monitoring est installé.

Pour chaque système où un agent Response Time Monitoring est installé, la page Configuration d'agent indique :

- Si le système est en ligne (coche sur fond vert) ou hors ligne (croix sur fond rouge).
- La version de l'agent Response Time Monitoring qui est installée.
- Si la configuration centrale ne parvient pas à déterminer le type de l'agent (c'est-à-dire si l'Analyseur de paquets ou le module IBM HTTP Server Response Time est utilisé pour surveiller des transactions HTTP), seul l'agent est rayé. En général, le type d'agent ne peut pas être déterminé lorsque l'agent n'envoie pas les détails associés via l'activité ASF.
- Si le système utilise les valeurs de configuration par défaut ou si des valeurs personnalisées sont définies.
- Les ports surveillés si l'agent Response Time Monitoring utilise l'Analyseur de paquets pour surveiller des transactions HTTP.

Setting	Value
Monitor HTTP traffic?	Yes
HTTP ports to monitor	80

- Si le module IBM HTTP Server Response Time, associé à l'agent HTTP Server, est utilisé pour surveiller les transactions HTTP.

Setting	Value
Is IBM HTTP Server Response Time module enabled?	Yes

Conseil : Le module IBM HTTP Server Response Time surveille automatiquement les transactions HTTP et HTTPS. Aucune configuration supplémentaire de l'agent Response Time Monitoring n'est obligatoire.

Sélectionnez un système pour afficher ses paramètres de configuration. Pour trouver un système spécifique, entrez son nom partiellement ou en entier dans la zone **Filter**.

Les personnalisations apportées à la page Configuration d'agent ont priorité sur les autres personnalisations et sur les valeurs par défaut.

Si vous changez d'avis concernant les paramètres modifiés, cliquez sur **Undo Changes** pour revenir aux paramètres dernièrement sauvegardés ou sur **Revert to Default** pour revenir aux valeurs par défaut.

Les nouvelles valeurs de configuration sont envoyées au composant Central Configuration Services et les agents en ligne sont alors automatiquement reconfigurés sans avoir à être redémarrés. Si l'agent est hors ligne, il télécharge les nouveaux paramètres de configuration lorsqu'il devient en ligne. Les données des nouveaux ports sont affichées dans les tableaux de bord associés à Response Time Monitoring lorsque les données sont actualisées.

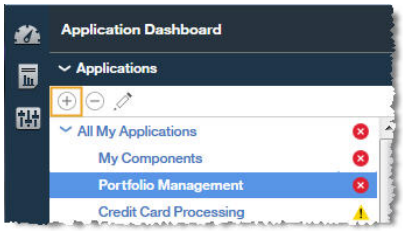
Ajout d'applications

Une fois que vous avez installé l'agent Response Time Monitoring, il se peut que vous deviez ajouter les applications à surveiller au Tableau de bord d'Application Performance.

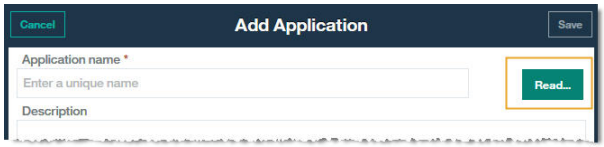
Procédure

Pour ajouter des applications au Tableau de bord d'Application Performance :

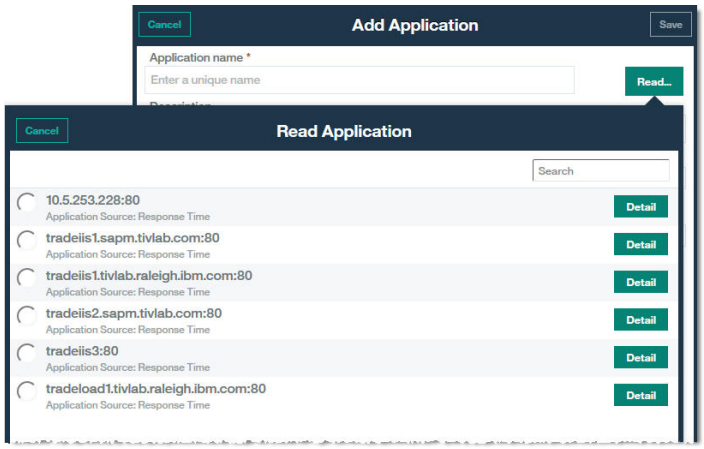
1. Dans le Tableau de bord d'Application Performance, cliquez sur **Ajouter une application**.



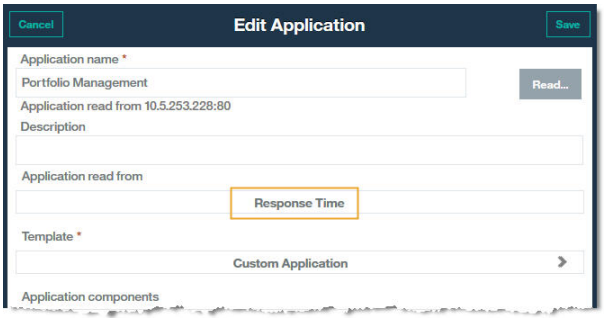
2. Sélectionnez **Lire** pour ouvrir la liste des applications reconnues.



3. Sélectionnez l'application à surveiller.



Temps de réponse s'affiche en tant que référentiel source dans la zone **Application lue dans** et les composants sont répertoriés dans **Composants d'application**.



4. Aucune configuration supplémentaire n'est requise pour afficher les applications surveillées par l'agent Response Time Monitoring dans le Tableau de bord d'Application Performance. Cliquez sur **Sauvegarder** dans la fenêtre Ajouter une application.

Résultats

Les applications détectées par l'agent Response Time Monitoring sont répertoriées dans **Toutes mes applications**, dans le Tableau de bord d'Application Performance.

Configuration du module IBM HTTP Server Response Time

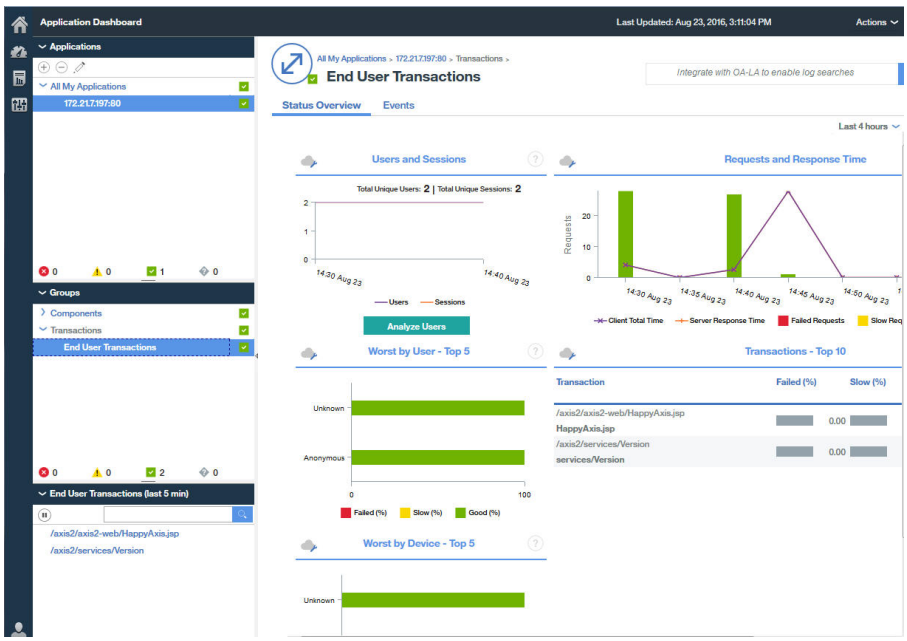
Pour IBM HTTP Server et Apache HTTP Server, utilisez le module IBM HTTP Server Response Time pour afficher les indicateurs réels de surveillance de temps de réponse de l'utilisateur final pour les pages HTTP.

Le module IBM HTTP Server Response Time est installé et configuré en tant qu'élément du agent HTTP Server. Le module IBM HTTP Server Response Time ne fonctionne qu'avec IBM HTTP Server et Apache HTTP Server sous AIX, Linux et Windows. Le module IBM HTTP Server Response Time surveille tous les ports pour les requêtes HTTP et HTTPS.

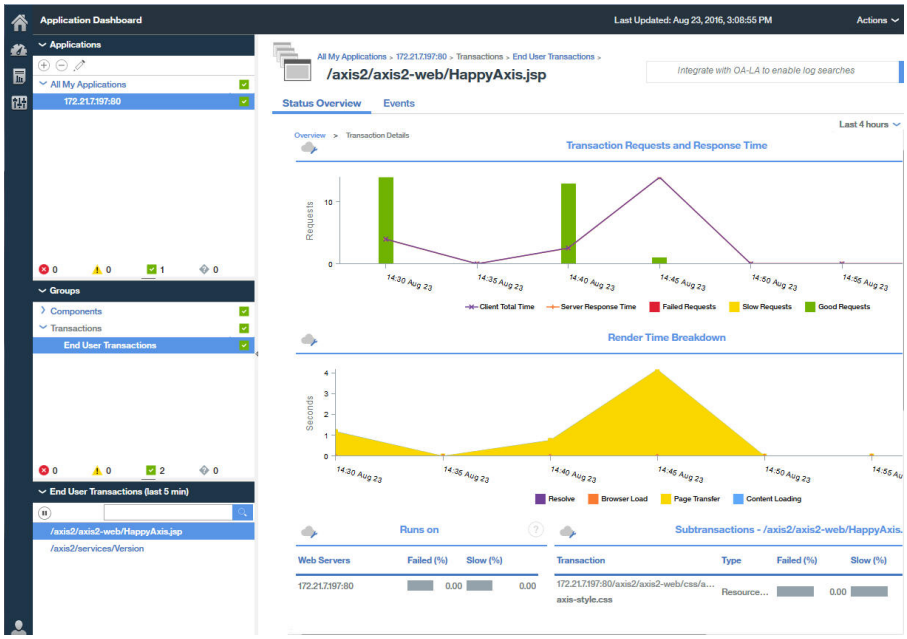
A l'aide de JavaScript, le module IBM HTTP Server Response Time insère un en-tête dans les pages Web transmises par IBM HTTP Server pour que l'agent de Response Time Monitoring puisse surveiller ces pages. Les objets imbriqués chargés par la page sont suivis à l'aide de cookies. Les informations de transaction des pages Web transmises par IBM HTTP Server ou Apache sont ensuite incluses dans les tableaux de bord Transactions utilisateur final.

Par exemple :

Espace de travail Transactions utilisateur final présentant les données collectées à partir du module IBM HTTP Server Response Time dans la section Transactions - 10 premières :



Espace de travail Transactions utilisateur final présentant les données collectées à partir du module IBM HTTP Server Response Time dans le tableau Sous-transactions



module IBM HTTP Server Response Time

Le module IBM HTTP Server Response Time fait partie de l'agent HTTP Server. Mais il fonctionne conjointement avec l'agent Response Time Monitoring pour surveiller les transactions d'application sur les serveurs HTTP pris en charge.

Lorsque vous installez l'agent Response Time Monitoring pour qu'il fonctionne avec le module IBM HTTP Server Response Time, il surveille les demandes HTTP et HTTPS sur tous les ports.

Le module IBM HTTP Server Response Time fait partie de l'agent HTTP Server. Vous devez installer l'agent HTTP Server soit avant l'agent Response Time Monitoring, soit en même temps.

L'agent HTTP Server est composé de deux plug-ins :

1. `khu_module` - correspond au agent HTTP Server. Ce plug-in est responsable de tous les tableaux de bord associés à l'agent HTTP Server. Pour plus d'informations, voir agent HTTP Server Reference.
2. `wrt_module` - correspond au module IBM HTTP Server Response Time.

Ces deux plug-ins sont indiqués dans le fichier de configuration de l'agent HTTP Server. Le fichier de configuration de l'agent HTTP Server est comme suit pour le serveur Apache HTTP Server :

```
khu.usr.local.apache24.conf.httpd.conf
```

Le fichier est comme suit pour le serveur IBM HTTP Server :

```
khu.opt.IBM.HTTPServer.conf.httpd.conf
```

La règle de nommage de ce fichier est : `khu.(chemin d'accès complet du fichier de conf du serveur http, remplacer le / par .).conf`

```
LoadModule khu_module
LoadModule wrt_module
```

Pour que le module IBM HTTP Server Response Time fonctionne, le fichier de configuration du serveur HTTP doit contenir une instructions include faisant référence au fichier de configuration du agent HTTP Server. Par exemple :

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Cette instruction include active les deux plug-ins en même temps. Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 319.

Installation et configuration du module IBM HTTP Server Response Time

La configuration est automatique du côté de l'agent Response Time Monitoring. Le module IBM HTTP Server Response Time doit être installé et configuré en tant qu'élément de l'agent HTTP Server. L'agent Response Time Monitoring détecte automatiquement le module IBM HTTP Server Response Time et l'active.

Pourquoi et quand exécuter cette tâche

Procédure

1. Installez l'agent HTTP Server qui installe automatiquement le module IBM HTTP Server Response Time.
2. Configurez l'agent HTTP Server. Cette opération active le module IBM HTTP Server Response Time. Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 319.
3. Installez l'Agent de surveillance des temps de réponse en tant que `superutilisateur` ou `Administrateur`, en fonction de votre système d'exploitation. Pour des instructions détaillées, voir Chapitre 9, «Installation des agents», à la page 161.
4. Redémarrez IBM HTTP Server. Lorsque le programme d'installation de Response Time Monitoring détecte l'agent HTTP Server, l'agent Response Time Monitoring active le module IBM HTTP Server Response Time automatiquement.

Activation manuelle du module IBM HTTP Server Response Time

Vous pouvez activer le module IBM HTTP Server Response Time manuellement afin de surveiller les performances des pages HTTP et des objets imbriqués des pages Web servies par IBM HTTP Server :

Pourquoi et quand exécuter cette tâche

Le module IBM HTTP Server Response Time est activé automatiquement lorsque l'eagent HTTP Server est installé et configuré. Toutefois, vous souhaiterez sans doute activer le module IBM HTTP Server Response Time manuellement.

Procédure

Pour activer le module IBM HTTP Server Response Time manuellement sous Linux, AIX ou Windows, procédez comme suit :

1. Linux AIX Pour activer le module IBM HTTP Server Response Time manuellement sous Linux ou AIX, procédez comme suit :
   a. Arrêtez l'agent Response Time Monitoring. Exécutez
      `$AGENT_HOME/bin/rt-agent.sh stop`

      où *$AGENT_HOME* peut correspondre à `/opt/ibm/apm/agent` sur un système Linux, ou à `/opt/ibm/ccm/agent` sur un système AIX.
   b. Exécutez une commande de configuration et utilisez *$AGENT_HOME*`/samples/rt_silent_config_ihs.txt` pour ajouter les modules de chargement au fichier de configuration de serveur Web et définissez les paramètres de configuration pour le module IBM HTTP Server Response Time.
   c. Redémarrez l'agent Response Time Monitoring.
2. Windows Pour activer le module IBM HTTP Server Response Time manuellement sous Windows, procédez comme suit :
   a. Arrêtez l'agent Response Time Monitoring. Exécutez
      REP_BASE_AGENT`\bin\rt-agent.bat stop`

      où *REP_BASE_AGENT* peut correspondre à `C:\IBM\APM` sur un système Windows.
   b. Exécutez une commande de configuration et utilisez *REP_BASE_AGENT*`\samples\rt_silent_config_ihs.txt` pour ajouter les modules de chargement au fichier de configuration de serveur Web et définissez les paramètres de configuration pour le module IBM HTTP Server Response Time. Par exemple,
      REP_BASE_AGENT`\bin\rt_agent.bat config` *REP_BASE_AGENT*`\samples\rt_silent_config_ihs.txt`
   c. Redémarrez l'agent Response Time Monitoring.

Désactivation manuelle du module IBM HTTP Server Response Time

Pour désactiver le module IBM HTTP Server Response Time et réutiliser l'Analyseur de paquets, reconfigurez l'agent et désactivez la surveillance du module IBM HTTP Server Response Time.

Pourquoi et quand exécuter cette tâche

Utilisez les procédures suivantes pour désactiver le module IBM HTTP Server Response Time.

Procédure

Pour reconfigurer l'agent en mode interactif sous Linux, AIX ou Windows, procédez comme suit :

1. Linux AIX Pour reconfigurer l'agent en mode interactif sous Linux et AIX, procédez comme suit :
   a. Exécutez *rép_install*`/bin/rt-agent.sh config`
      Où *rép_install* correspond à `/opt/ibm/apm/agent` sous Linux et AIX.
   b. Redémarrez l'agent Response Time Monitoring.

   Sinon, pour définir les paramètres manuellement :
   a. Ouvrez *rép_install*`/config/`*nom_hôte*`_t5.cfg` dans un éditeur de texte.
      où *rép_install* correspond à `/opt/ibm/apm/agent` sous Linux et AIX.
   b. Définissez les paramètres suivants :
      ```
      KT5DISABLEANALYZER=NO
      KT5ENABLEWEBPLUGIN=NO
      ```
   c. Redémarrez l'agent Response Time Monitoring.

2. Windows Pour reconfigurer l'agent en mode interactif sous Windows, procédez comme suit :
   a. Pour définir manuellement les paramètres connexes, ouvrez le fichier *rép_install*\TMAITM6_x64\<nomhôte>_t5.cfg dans un éditeur de texte. où *rép_install* correspond à C:\IBM\APM sous Windows.
   b. Définissez les paramètres suivants :
      ```
      KT5DISABLEANALYZER=NO
      KT5ENABLEWEBPLUGIN=NO
      ```
   c. Redémarrez l'agent Response Time Monitoring.

Configuration avancée du module IBM HTTP Server Response Time

Il existe un certain nombre d'options de configuration avancées pour le module IBM HTTP Server Response Time.

Le module IBM HTTP Server Response Time est configuré automatiquement, mais il existe certaines tâches de configuration avancées que vous pouvez effectuer pour affiner les performances et les fonctionnalités.

Désactivation de la surveillance de la temporisation des ressources :

La surveillance de la temporisation des ressources est activée pour toutes les instances du module IBM HTTP Server Response Time installées par l'agent HTTP Server.

Pourquoi et quand exécuter cette tâche

Pour réduire le nombre de ressources surveillées par le module IBM HTTP Server Response Time ou désactiver la surveillance de la temporisation des ressources afin de réduire la charge de traitement requise pour surveiller une instance spécifique d'IBM HTTP Server, éditez le fichier de configuration généré de l'agent HTTP Server (*nom_hôte_port*.conf).

Procédure

Pour modifier le fichier de configuration de l'agent HTTP Server, procédez comme suit :

1. Ouvrez le fichier de configuration de l'agent HTTP Server dans un éditeur de texte. Par exemple, /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
2. Ajoutez la ligne WrtMaxPostResourcesSize. Définissez l'une des valeurs suivantes :
   - WrtMaxPostResourcesSize -1 pour surveiller toutes les ressources.
   - WrtMaxPostResourcesSize 0 pour désactiver la surveillance des ressources.
   - WrtMaxPostResourcesSize *n* pour surveiller un nombre de ressources spécifique, 10 par défaut. Par exemple, définissez WrtMaxPostResourcesSize 2 pour définir deux ressources au maximum à envoyer au serveur.
3. Redémarrez le serveur.

Désactivation de la génération de corrélateur ARM :

Par défaut, la génération de corrélateur ARM Correlator est activée, ce qui permet au module IBM HTTP Server Response Time de se connecter à tous les serveurs d'arrière-plan de la topologie. Vous pouvez désactiver la génération de corrélateur ARM Correlator si nécessaire.

Pourquoi et quand exécuter cette tâche

Restriction : Si vous désactivez la génération de corrélateur ARM, le module IBM HTTP Server Response Time ne peut pas établir de liaison avec les serveurs d'arrière-plan, comme WebSphere Application Server. Désactivez-la uniquement sur conseil du service de support logiciel IBM.

Procédure

Pour désactiver la génération de corrélateur ARM, procédez comme suit :

1. Ouvrez le fichier de configuration de l'agent HTTP Server dans un éditeur de texte. Par exemple, `opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf`
2. Ajoutez la ligne suivante :
   ```
   WrtDisableArmCorr
   ```

Contournement du cookie WRTCorrelator :

Si l'injection JavaScript est activée pour l'agent Response Time Monitoring sur WebSphere Portal, les cookies tels que le cookie WRTCorrelator risquent d'être à l'origine de problèmes lors de l'utilisation de WebSphere Portal. Pour éviter ces problèmes, vous pouvez définir le cookie WRTCorrelator sur ignore.

Procédure

1. Si nécessaire, démarrez le serveur `WebSphere_Portal`.
2. Connectez-vous à WebSphere Integrated Solutions Console.
3. Accédez à **Ressources** > **Environnement de ressources** > **Fournisseurs d'environnement de ressources**.
4. Sélectionnez **WP ConfigService**.
5. Sous Propriétés supplémentaires, sélectionnez **Propriétés personnalisées**.
6. Cliquez sur **Nouveau**.
7. Spécifiez le nom de la propriété (le cookie WRTCorrelator dans le cas présent), puis définissez la valeur de cette propriété sur ignore. Pour définir le cookie WRTCorrelator sur ignore, entrez ce qui suit :
   ```
   cookie.ignore.regex =
   digest\.ignore.*|LTPAToken|LTPAToken2|JSESSIONID|WASReqURL|WRTCorrelator
   |PD_STATEFUL.*
   ```
8. Cliquez sur **Appliquer** et sauvegardez vos modifications.
9. Déconnectez-vous de WebSphere Integrated Solutions Console.

Résultats

Le cookie WRTCorrelator est défini sur ignore et les problèmes tels que les conditions de fin de boucle sont évités.

Exclusion de pages de la génération de rapports du temps client :

Vous pouvez exclure des pages particulières de la génération de rapports du temps client à partir du navigateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter un paramètre dans le fichier de configuration pour que le module IBM HTTP Server Response Time arrête d'injecter du code JavaScript dans un fichier qui correspond aux modèles que vous spécifiez. Cela arrête la génération de rapports de temps client à partir du navigateur pour ces pages.

Procédure

Pour exclure des pages particulières de la génération de rapports du temps client à partir du navigateur, procédez comme suit :

1. Dans la section **advconfig** du fichier `$AGENT_HOME/config/nomhôte_t5.cfg`, ajoutez :
   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=URL_path_pattern to_exclude}
   ```

Par exemple,

```
{KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=*/DoNotJSIMe.jsp,/absolutePath/index.jsp,/skipThisDir/*}
```

Conseil : Utilisez un astérisque (*) comme préfixe ou suffixe pour correspondre aux modèles. Ajoutez plusieurs valeurs séparées par une virgule au paramètre si nécessaire.

2. Redémarrez l'agent Response Time Monitoring. Exécutez les commandes suivantes :

```
rt-agent.sh stop
rt-agent.sh start
```

Utilisation du module IBM HTTP Server Response Time en tant qu'utilisateur non superutilisateur :

En prenant un certain nombre de précautions lors de la configuration, vous pouvez utiliser le module IBM HTTP Server Response Time avec un ID utilisateur autre que l'ID superutilisateur (`root`). Si vous utilisez Network Analyseur de paquets, notez que vous devez utiliser l'ID `root`.

Pour utiliser un ID utilisateur autre que l'ID `root`, procédez comme suit :

Pour l'agent Response Time Monitoring

Installez l'agent Response Time Monitoring dans un répertoire doté d'un accès en écriture, à l'aide de l'ID utilisateur avec lequel vous allez l'exécuter.

- Pour cette procédure, l'ID utilisateur de l'agent Response Time Monitoring est *agentuser*. Le répertoire dans lequel l'agent est installé est *$AGENT_HOME*.
- Si vous installez l'agent Response Time Monitoring en tant qu'utilisateur `root` et que vous exécutez ensuite l'agent à l'aide d'un autre ID utilisateur, vous ne pourrez pas créer de fichiers.

Pour le module IBM HTTP Server Response Time

`ServerRoot` doit appartenir au même ID utilisateur que celui utilisé pour exécuter `apache start|stop`.

- Lors de l'exécution de la commande `apache start`, le répertoire de suivi `wrt` est créé sous `ServerRoot`. L'utilisateur doit disposer de droits suffisants pour créer des fichiers et des répertoires sous `ServerRoot`.
- Si l'utilisateur du module IBM HTTP Server Response Time, *ihsuser*, est différent de l'utilisateur *agentuser*, il requiert un accès en écriture dans `$AGENT_HOME/tmp`.

  `$AGENT_HOME/tmp` est créé lors de l'installation d'agents. L'ID utilisateur *ihsuser* doit être autorisé à créer le répertoire `kt5` dans `$AGENT_HOME/tmp`.
- Il peut y avoir plusieurs versions de `ServerRoot`, chacune administrée par des utilisateurs différents.

Pour l'agent Response Time Monitoring et le module IBM HTTP Server Response Time

Les ID utilisateur *agentuser* et *ihsuser* doivent disposer d'un accès en lecture/écriture dans les répertoires suivants :

- `$AGENT_HOME/tmp/kt5`
- `ServerRoot/wrt`

En général, le module IBM HTTP Server Response Time est démarré en premier et les répertoires `wrt` sont créés automatiquement par Response Time Monitoring lors de son premier démarrage avec des droits en lecture/écriture pour tous.

`ServerRoot/wrt` est également utilisé par `camconfig` pour transmettre la configuration. L'utilisateur *ihsuser* crée des fichiers d'ID de file d'attente partagés qui sont sélectionnés par l'utilisateur *agentuser* ; l'utilisateur *agentuser* lit l'ID de file d'attente dans le répertoire et transmet la configuration.

Si `root` est utilisé pour exécuter initialement `apache start` et que *ihsuser* n'est pas `root`, procédez comme suit :

1. Arrêtez l'agent Response Time Monitoring.
2. En tant qu'utilisateur `root`, exécutez `apachectl stop`.
3. Supprimez les répertoires suivants :
   - `$AGENT_HOME/tmp/kt5`
   - `ServerRoot/wrt`
4. En tant qu'utilisateur *ihsuser*, exécutez `apachectl start` pour recréer les répertoires avec les droits appropriés.

Pour réinitialiser les droits de l'module IBM HTTP Server Response Time dans le répertoire `wrt`

Vous pouvez réinitialiser les droits du répertoire `wrt` de l'module IBM HTTP Server Response Time pour plus de sécurité. La mise à jour implique l'ajout d'un paramètre dans le fichier de configuration pour limiter les droits d'accès au répertoire `wrt` créé par l'utilisateur non root lors de l'installation de IBM HTTP Server.

Effectuez cette procédure sur le système sur lequel le module IBM HTTP Server Response Time est installé pour modifier les droits du répertoire `wrt` pour l'utilisateur non root de 777 en 700 :

1. Ouvrez le fichier `$IHS_HOME$/conf/httpd.conf` dans un éditeur de texte.
2. Ajoutez la propriété **`WrtDisableDirPermNonRoot`** à la fin du fichier :
   - Si cette propriété est activée, seul l'ID utilisateur ayant démarré httpd et correspondant à l'ID utilisateur ayant créé le répertoire est utilisé pour créer le répertoire `wrt` avec les droits 700. L'accès à ce répertoire est refusé à tous les autres utilisateurs.
   - Si cette propriété n'est pas activée, le répertoire `wrt` est créé avec les droits par défaut 777.
3. Redémarrez l'agent Response Time Monitoring :

```
rt-agent.sh stop
rt-agent.sh.start
```

Les données de configuration Response Time Monitoring et certains fichiers persistants sont stockés dans le répertoire `wrt`, qui est utilisé lors du processus de communication, et chaque processus de connexion y crée un fichier de configuration wrt. Une fois que vous avez ajouté **`WrtDisableDirPermNonRoot`** au fichier `httpd.conf`, seuls certains utilisateurs peuvent communiquer avec l'agent de surveillance Response Time Monitoring.

Utilisation des équilibreurs de charge :

Si vous utilisez des équilibreurs de charge dans votre environnement, il est nécessaire de les personnaliser.

Procédure

Si vous utilisez un équilibreur de charge, procédez comme suit :

1. Désactivez la réécriture des URL sur l'équilibreur de charge.
2. Installez un agent Response Time Monitoring sur chaque serveur Web que vous souhaitez surveiller. N'installez pas Response Time Monitoring sur l'équilibreur de charge.

Que faire ensuite

Si vous exécutez l'agent Response Time Monitoring derrière un équilibreur de charge, vous pouvez configurer ce dernier afin qu'il achemine l'adresse IP du client pour optimiser les performances de surveillance. Utilisez les étapes suivantes comme exemple :

1. Dans l'en-tête HTTP, définissez l'adresse IP du client dans la zone **`X-Forwarded-For`**.
2. Dans le fichier `$AGENT_HOME/config/`*`nom_hôte`*`_t5.cfg`, ajoutez `{KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=X-Forwarded-For}` à la section `SECTION=advconfig`.

Conseil : Ajoutez plusieurs valeurs au paramètre si nécessaire. Par exemple, `{KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=x-forwarded-for, iv-remote-address}`

3. Redémarrez l'agent Response Time Monitoring. Exécutez les commandes suivantes :

```
rt-agent.sh stop
rt-agent.sh start
```

Limitation de l'UC utilisée pour surveiller IBM HTTP Server :

Dans des environnements saturés, vous pouvez être amené à limiter le pourcentage d'unité centrale utilisé par l'instrumentation IBM HTTP Server.

Pourquoi et quand exécuter cette tâche

Indiquez le pourcentage d'unité centrale que le module IBM HTTP Server Response Time peut utiliser. Le pourcentage d'unité centrale utilisé n'est pas limité par défaut. Configurez le pourcentage d'unité centrale sur le serveur où l'agent est installé.

Procédure

Pour configurer le pourcentage d'unité centrale utilisée, procédez comme suit :

1. Vous pouvez effectuer l'une des actions suivantes :
   a. Reconfigurez l'agent en mode interactif ; exécutez :
      `$AGENT_HOME/bin/rt-agent.sh config`
   b. Ouvrez le fichier *rép_install*`/config/`*hostname*`_t5.cfg`

   Où *rép_install* correspond à `/opt/ibm/apm/agent` sous Linux et AIX.
2. Dans la section **advconfig**, définissez la valeur 0-100 pour le paramètre suivant :
   `KT5WEBPLUGIN_TARGET_CPU_PERCENTAGE=`*10*

   Où la valeur que vous indiquez est le pourcentage limite d'utilisation de l'unité centrale. La valeur par défaut *0* signifie que l'utilisation de l'unité centrale n'est pas limitée.
3. Facultatif : Si vous êtes un utilisateur avancé, vous pouvez également définir les paramètres suivants :

Option	Description
KT5WEBPLUGINCONFIGPOSTURL	Liste d'URL correspondant à une installation d'IBM HTTP Server. Valeur par défaut : `http://localhost/WrtUpdateConfig.dat`
KT5WEBPLUGIN_MAX_REQUESTS_PER_SECOND	Nombre de demandes par seconde surveillé par chaque installation d'IBM HTTP Server. Si le nombre de demandes dépasse ce chiffre, les demandes ultérieures ne sont pas surveillées. Si la limite est atteinte, l'insertion de JavaScript s'arrête, et aucune donnée n'est renvoyée à l'agent Response Time Monitoring. Valeur par défaut : `0` (aucun maximum)
KT5WEBPLUGIN_CPUMAN_PERIOD_IN_SEC	Période en secondes pendant laquelle l'utilisation de l'unité centrale est vérifiée pour déterminer si la cible a été dépassée. Valeur par défaut : `60` secondes

Option	Description
KT5WEBPLUGIN_CATCHUP_PERIOD_COUNT	Nombre de périodes autorisées dans le même état avant que l'utilisation de l'unité centrale soit réduite. Par exemple, avec la valeur par défaut, si l'utilisation de l'unité centrale est élevée et le reste quatre cycles plus tard, elle est réduite. Valeur par défaut : 3

Résultats

Le pourcentage d'unité centrale à la disposition du module IBM HTTP Server Response Time est défini sur une valeur fixe.

Organigramme de l'Analyseur de paquets

Utilisez l'Analyseur de paquets pour surveiller les transactions HTTP. Vous devrez configurer manuellement la surveillance HTTPS. Vous devrez instrumenter manuellement vos pages Web pour la collecte des temps du navigateur.

Pour déterminer les environnements dans lesquels vous pouvez utiliser l'Analyseur de paquets, consultez «Response Time Monitoring Composants», à la page 639 et «Planification de l'installation», à la page 640.

L'Analyseur de paquets est automatiquement activé lorsque vous installez l'agent de Response Time Monitoring, mais vous devrez peut-être effectuer un certain nombre d'étapes et personnalisations supplémentaires.

1. Vous pouvez personnaliser les paramètres de l'Analyseur de paquets, par exemple, le numéro de port dans la fenêtre Configuration d'agent. Pour plus d'informations, voir «Configuration de Analyseur de paquets à l'aide de la fenêtre Configuration d'agent».
2. Pour surveiller les transactions HTTPS, vous devrez instrumenter manuellement vos pages Web pour la collecte des temps du navigateur. Pour plus d'informations, voir «Surveillance des transactions HTTPS», à la page 658.
3. Pour activer les temps du navigateur, ajoutez le composant d'injection JavaScript et associez le composant de surveillance JavaScript à votre application. Pour plus d'informations, consultez «Ajout du composant de surveillance JavaScript à votre application», à la page 657.
4. Si vous utilisez un environnement où les charges de transactions sont élevées, vous aurez peut-être besoin d'effectuer des étapes d'optimisation avancées. Pour plus d'informations, voir «Configuration avancée de Packet Analyzer», à la page 662

Configuration de Analyseur de paquets à l'aide de la fenêtre Configuration d'agent

Vous pouvez utiliser la fenêtre Configuration d'agent pour configurer Analyseur de paquets.

Pour surveiller le trafic HTTP d'un système spécifique à l'aide de l'Analyseur de paquets, procédez comme suit :

1. Pour accéder à la page Configuration d'agent, dans l'Interface graphique APM , sélectionnez **Configuration du système** > **Configuration d'agent**, puis l'onglet **Temps de réponse**.
2. Sélectionnez le(s) système(s) que vous souhaitez mettre à jour. Sélectionnez plusieurs systèmes si vous souhaitez utiliser les mêmes paramètres HTTP pour chacun de ces systèmes.

   Si les systèmes que vous sélectionnez ont des valeurs HTTP définies qui sont différentes, `Multiple Values` ou `Multiple Lists` s'affiche à la place des valeurs individuelles. Vous ne pouvez pas mettre à jour simultanément des systèmes avec des valeurs différentes.
3. Dans la zone **Monitor HTTP traffic?**, cliquez deux fois sur la valeur et sélectionnez **Yes** dans la liste.

4. Dans la zone **Ports HTTP à surveiller**, cliquez deux fois sur la valeur et entrez les ports supplémentaires que vous souhaitez surveiller, à l'exception du port par défaut 80 et des autres ports déjà répertoriés.

   Pour arrêter la surveillance d'un port, sélectionnez le port que vous ne souhaitez plus surveiller et cliquez sur **Supprimer**.
5. Cliquez sur **Appliquer les modifications**.

Ajout du composant de surveillance JavaScript à votre application

Pour vous permettre de comprendre les performances de vos pages Web dans un navigateur, ainsi que les erreurs, l'agent Response Time Monitoring doit pouvoir collecter les données de temporisation du navigateur. Pour activer cette fonction, vous devez configurer l'application que vous voulez surveiller.

Pourquoi et quand exécuter cette tâche

Avant de pouvoir surveiller les interactions dans vos pages Web, vous devez ajouter le composant de surveillance JavaScript à chaque page Web pour votre application. Le composant de surveillance JavaScript capture l'état de chaque page Web et de leurs interactions JavaScript associées. Ajoutez le composant de surveillance JavaScript à l'application que vous voulez surveiller. Le contenu et les actions appropriés sont automatiquement capturés et envoyés au serveur Cloud APM à des fins d'analyse et de corrélation.

Procédure

Pour activer la collecte des données de surveillance utilisateur réelles à partir du navigateur, procédez comme indiqué ci-après. Ces étapes ne doivent être exécutées qu'une seule fois, sauf si la configuration de l'application change.

1. Ajoutez le composant de surveillance JavaScript à l'application. La procédure à utiliser dépend du type d'application :
   a. Pour les applications Java EE, extrayez *rép_installation*/clienttime/ClientTime.war depuis le module d'installation vers un répertoire auquel le serveur HTTP peut accéder.
   b. Pour les applications autres que les applications non Java EE, par exemple Ruby, .NET, Python et Node.js, sauvegardez *rép_install*/clienttime/wrtInstrumentation.js depuis le module d'installation dans un répertoire auquel le serveur HTTP peut accéder.
2. Associez le composant de surveillance JavaScript à l'application.

   Normalement, vous pouvez effectuer cette association en modifiant un script d'en-tête d'application. En général, il suffit de modifier un script d'en-tête seulement pour chaque composant ou application à surveiller.

   Pour les applications Java EE et non Java EE, ajoutez le code JavaScript suivant à l'en-tête d'application, avant tout autre code JavaScript :

   ```
   <script language="JavaScript" src="chemin/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   ```

   où *chemin* est le chemin d'accès relatif au composant de surveillance JavaScript.

   Par exemple :

   ```
   <script language="JavaScript" src="/ClientTime/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   ```

Résultats

Les pages qui sont instrumentées avec le composant de surveillance JavaScript sont surveillées, et les données provenant de ces pages sont analysées et affichées dans des tableaux de bord Transactions utilisateur final.

Activation des temps du navigateur :

En activant la surveillance de la temporisation des ressources, l'agent Response Time Monitoring traite les données de temporisation des ressources W3C à l'aide de l'Analyseur de paquets. Si cette fonction est activée, vous pouvez afficher des informations détaillées sur les performances des éléments en avant-plan.

Pourquoi et quand exécuter cette tâche

Pour pouvoir surveiller les données de temporisation des ressources, vous devez ajouter le composant de surveillance de la temporisation des ressources à votre application et l'associer à votre application. Le composant de surveillance de la temporisation des ressources capture automatiquement l'état et les interactions des éléments en avant-plan et envoie les données au serveur Cloud APM pour analyse. Les résultats de cette analyse sont affichés dans le tableau de bord **Sous-transactions**.

Procédure

Effectuez les étapes ci-après pour activer la fonction de surveillance de la temporisation des ressources. N'effectuez ces étapes qu'une seule fois, sauf si la configuration de l'application change.

1. Ajoutez le composant de surveillance de la temporisation des ressources à l'application.
   a. Extrayez le fichier *rép_install*`/clienttime/wrtInstrumentation.js` du package d'installation.
   b. Ajoutez le fichier `wrtInstrumentation.js` au répertoire JavaScript de votre application.
2. Ajoutez la ligne suivante à l'en-tête d'application :

   ```
   <script> var wrt_enableResourceTiming=true; </script>
   ```

   Par exemple,

   ```
   <script language="JavaScript" src="chemin/wrtInstrumentation.js"
   type="text/JavaScript"></script><script> var wrt_enableResourceTiming=true; </script>
   ```

Résultats

Les pages sont instrumentées avec le composant de surveillance de la temporisation des ressources. Ce composant est activé par défaut. Les données de temporisation des ressources sur les pages instrumentées avec le composant de surveillance de la temporisation des ressources sont analysées et affichées dans les tableaux de bord **Sous-transactions**.

Que faire ensuite

Si vous souhaitez désactiver le composant de surveillance de la temporisation des ressources, définissez le paramètre **`wrt_enableResourceTiming`** sur `false`.

Surveillance des transactions HTTPS

Response Time Monitoring surveille par défaut les transactions HTTPS. Pour surveiller des transactions HTTPS, Response Time Monitoring a besoin d'accéder aux certificats SSL afin de déchiffrer le trafic SSL provenant de vos serveurs Web distants.

Avant de commencer

Identifiez les serveurs Web HTTPS à surveiller, y compris leurs adresses IP et les ports configurés. Par exemple, `192.168.1.23`, port `443`. Pour chaque serveur Web HTTPS, vérifiez que Response Time Monitoring peut lire ses chiffrements. Response Time Monitoring prend en charge les chiffrements pris en charge par IBM Java et notamment les chiffrements ci-après.

- RSA_WITH_RC4_40_MD5
- RSA_WITH_RC4_128_MD5
- RSA_WITH_RC4_128_SHA

- RSA_WITH_RC4_40_SHA
- RSA_WITH_DES40_CBC_SHA
- RSA_WITH_DESC_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_MD5
- RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
- RSA_EXPORT1024_WITH_DES_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Restriction : Response Time Monitoring ne peut pas déchiffrer le trafic qui utilise l'échange de clés Diffie-Hellman.

Procédure

Pour activer la surveillance des transactions HTTPS, procédez comme suit :

1. Configurez le magasin de clés. Pour plus d'informations, voir «Configuration du magasin de clés», à la page 660.
2. Configurez l'agent Response Time Monitoring en exécutant l'une des commandes suivantes et en fournissant les valeurs demandées : Par exemple :

```
Configuring Response Time Monitoring Agent
Edit 'Response Time Monitoring Agent' settings? [1=Yes,2=No](default is: 1): 1

Basic Configuration :   Specify basic monitoring configuration. Note: HTTP is
now configured centrally using the Response Time tab under Agent Configuration.

Specifies if HTTPS transactions should be monitored
Monitor HTTPS transactions [ 1=Yes, 2=No ] (default is:2): 1

This keystore contains the certificates of the HTTPS websites being monitored
HTTPS keystore (e.g. - /tmp/keys.kdb) (default is: ): /tmp/keys.kdb

This table maps HTTPS servers to the appropriate certificates (e.g. cert1,
server ip,server port; cert2,server2 ip,server2 port);...
HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)(default is: ):
 label1,10.0.0.1,9443;label1,9.185.150.71,443

Advanced Configuration :
Specify advanced monitoring configuration

The NIC card which has the selected IP address will be monitored.
IP address of the NIC to be monitored (default is: ): 10.0.0.1

Data Collection and Analysis Configuration :
Specify Configuration Information on how Data is Analyzed.

Configuration completed successfully.
Agent restart required to apply configuration changes.
```

   Où :

   - Le magasin de clés HTTPS est le magasin de clés configuré à l'étape 1
   - Pour la mappe de certificat serveur HTTPS, indiquez :
     - `label 1` : Libellé de clé configuré à l'étape 1

– `server ip` : Adresse IP du serveur, qui doit correspondre à l'attribut Source/Destination dans l'en-tête IPV4 des paquets
– `server port` : Numéro de port du serveur, qui doit correspondre à l'attribut Source/Destination port dans l'en-tête TCP des paquets

Ajoutez plusieurs entrées pour plusieurs possibilités de l'IP de serveur du même intitulé de clé.

- adresse IP de la carte d'interface réseau à surveiller, l'interface qui peut voir les paquets et qui est mappée à eth0, en0, etc. Le nom n'a pas besoin de correspondre à l'un des attributs des en-têtes IPV4 ou TCP des paquets. Si `10.0.0.1` correspond à eth0, utilisez `tcpdump -s0 -i eth0 ...` pour afficher tous les paquets que doit analyser l'analyseur de paquets.

3. Redémarrez l'agent Response Time Monitoring.

Configuration du magasin de clés :

Pour surveiller des transactions HTTPS, importez des clés dans KT5Keystore pour tous les serveurs Web que vous voulez surveiller.

Pourquoi et quand exécuter cette tâche

Vous pouvez exporter les certificats SSL à partir des serveurs Web que vous surveillez et les importer dans le magasin de clés HTTPS à l'aide d'IBM Key Management (iKeyman) ou spécifier le fichier de dissimulation du serveur Web (`.kdb`) dans le magasin de clés HTTPS. Lorsque vous installez ou configurez Response Time Monitoring, vous êtes invité à entrer l'emplacement du fichier `keys.kdb`.

Si vous ne disposez pas des fichiers de dissimulation de magasin de clés (`.kdb` et `.sth`), vérifiez si le fournisseur CMS est activé dans votre version Java pour que vous puissiez utiliser iKeyman pour définir la base de données de clés :

1. Accédez au répertoire *rép_install*`/ibm-jre/jre/lib/security`. Exemple :
   - Linux `/opt/ibm/apm/agent/JRE/lx8266/lib/security`
   - Windows `C:\Program Files\IBM\APM\ibm-jre\jre\lib\security`
2. Dans le fichier `java.security`, ajoutez l'instruction ci-après à la liste des fournisseurs de sécurité, comme indiqué, où *numéro* est le dernier numéro de séquence dans la liste.

   ```
   security.provider.numéro=com.ibm.security.cmskeystore.CMSProvider
   ```

   La liste des fournisseurs est similaire à celle de l'exemple suivant :

   ```
   ## List of providers and their preference orders #
   security.provider.1=com.ibm.jsse.IBMJSSEProvider
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.4=com.ibm.security.cert.IBMCertPath
   security.provider.5=com.ibm.security.cmskeystore.CMSProvider
   ...
   #
   ```

3. Sauvegardez et fermez le fichier.

Restriction : Response Time Monitoring ne peut pas déchiffrer le trafic à l'aide de l'échange de clés Diffie-Hellman.

Procédure

Pour activer la surveillance des transactions HTTPS, collectez les certificats SSL à partir des serveurs Web à surveiller et importez ces certificats, ainsi que les fichiers de dissimulation du magasin de clés dans le magasin de clés HTTPS, à l'aide d'iKeyMan. L'exemple suivant utilise iKeyman pour exporter les certificats d'un serveur IBM HTTP Server, puis les importer dans le magasin de clés HTTPS :

1. Installez un agent Response Time Monitoring sur chaque serveur Web HTTPS à surveiller.

2. Exécutez **IBM Key Management** (iKeyman) à partir du répertoire `bin` d'IBM Java en exécutant l'une des commandes ci-après, en fonction de votre système d'exploitation.
   - AIX Linux `/opt/ibm/apm/agent/JRE/lx8266/bin/ikeyman`

     Remarque : X-Window doit être installé dans l'environnement pour qu'iKeyMan fonctionne correctement.
   - Windows `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`
3. Créez une base de données de magasin de clés. Dans la boîte de dialogue **Nouveau**, procédez comme suit :
   a. Dans la liste **Key database type**, sélectionnez **CMS**. Si CMS n'est pas disponible dans la liste, le fournisseur CMS n'est peut-être pas activé. Activez le fournisseur CMS dans le fichier de sécurité Java.
   b. Dans la zone **Nom du fichier**, entrez le nom du fichier de clé HTTPS et cliquez sur **OK**. Par exemple, `keys.kdb`.
4. Dans la boîte de dialogue **Password Prompt**, procédez comme suit :
   a. Dans les zones **Password** et **Confirm Password**, entrez et confirmez le mot de passe d'accès à `keys.kdb`. Ne définissez pas de délai d'expiration sauf si vous souhaitez régulièrement recréer la base de données de clés et redémarrer l'agent Response Time Monitoring.
   b. Sélectionnez **Stash the password to a file?** pour stocker le mot de passe de `keys.kdb` sous forme chiffrée dans un fichier de dissimulation, `keys.sth`.
5. Dans la section **Key database content** de la fenêtre iKeyman, procédez comme suit :
   a. Sélectionnez **Personal Certificates**.
   b. Cliquez sur **Import**.
   c. Dans la boîte de dialogue **Import Key**, dans la liste **Keyfile type**, sélectionnez **CMS**.
   d. Parcourez le fichier de clés et cliquez sur **Open**, puis sur **OK**.
   e. Dans la boîte de dialogue **Password Prompt**, entrez le mot de passe du magasin de clés.
   f. Sélectionnez la clé dans la liste et cliquez sur **OK**.
   g. Dans la boîte de dialogue **Change Labels**, sélectionnez le nom de libellé de la clé. Dans la zone **Enter a new label**, indiquez le nom d'hôte du serveur et cliquez sur **Apply**.

      Remarque : Cette valeur sera nécessaire lorsque vous configurerez Response Time Monitoring, notez-la.
   h. Cliquez sur **OK**.
6. Sauvegardez le magasin de clés HTTPS.

Importation de clés depuis Internet Information Services

Pour extraire des clés d'Internet Information Services et les importer dans KT5Keystore, procédez comme suit :

1. Installez un agent Response Time Monitoring sur chaque serveur Web HTTPS à surveiller.
2. Exportez un fichier .pfx à partir d'Internet Information Services :
   a. Dans le menu **Démarrer** de Windows, sélectionnez **Outils d'administration** > **Gestionnaire des services Internet (IIS)**.
   b. Sélectionnez le serveur Web et le site dont vous souhaitez exporter la clé privée, puis cliquez avec le bouton droit de la souris et sélectionnez **Propriétés** dans le menu contextuel.
   c. Sélectionnez l'onglet **Sécurité de répertoire**, puis sélectionnez **Certificat du serveur** dans la section **Communications sécurisées**.
   d. Dans **Assistant Certificat d'IIS**, cliquez sur **Suivant**.
   e. Sélectionnez **Exporter le certificat actuel vers un fichier .pfx**, puis cliquez sur **Suivant**.

f. Entrez le chemin d'accès et le nom de fichier, puis cliquez sur **Suivant**.
g. Entrez un mot de passe d'exportation pour la clé, puis cliquez sur **Suivant**.
h. Cliquez sur **Suivant** sur toutes les pages suivantes, puis cliquez sur **Terminer**.

3. Procédez à l'extraction des certificats personnels et de signataires à partir du fichier .pfx :
   a. Exécutez **IBM Key Management** (iKeyman) à partir du répertoire `bin` d'IBM Java à l'aide de la commande `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`. Vérifiez que la variable d'environnement `JAVA_HOME` est définie.
   b. Dans la base de données de fichiers de clés, sélectionnez **Fichier** > **Ouvrir**.
   c. Dans la liste **Key database type**, sélectionnez **PKCS12**.
   d. Entrez le nom et le chemin d'accès du fichier de .pfx précédemment créé, puis cliquez sur **OK**. A l'invite, entrez le mot de passe, puis cliquez sur **OK**.
   e. Sélectionnez **Key Database Content** > **Personal Certificates**, puis cliquez sur **Export/Import**.
   f. Sélectionnez le type d'action **Exporter la clé** et le type de fichier de clés **PKCS12**. Entrez un nom de fichier et un emplacement pour la clé exportée, puis cliquez sur **OK**. A l'invite, entrez un mot de passe d'exportation puis cliquez à nouveau sur **OK**.
   g. Si le certificat personnel a été signé par une autorité de certification, sélectionnez **Key Database Content** > **Signer Certificates**, puis cliquez sur **Extract**. Sélectionnez le type de fichier par défaut, et entrez un nom de fichier et un emplacement pour le certificat exporté, puis cliquez sur **OK**.
4. Procédez à l'extraction des fichiers de signataire `.cer` (si nécessaire) :
   a. Si un fichier de certificats de signataire a été extrait du fichier .pfx, accédez au répertoire dans lequel il a été sauvegardé et effectuez une nouvelle copie avec l'extension `.cer`. Cliquez deux fois sur la nouvelle copie pour l'ouvrir à l'aide de l'afficheur de certificats Windows.
   b. Dans l'onglet **Chemin d'accès de certification**, vous pouvez afficher la chaîne de certificats de signataire. L'élément le plus bas de la chaîne doit être le certificat personnel. Pour tous les certificats au-dessus, procédez comme suit :
      1) Sélectionnez un certificat et cliquez sur **Afficher le certificat**.
      2) Sélectionnez **Détails** et cliquez sur **Copier dans un fichier**.
      3) Acceptez toutes les valeurs par défaut dans l'assistant d'exportation de certificat et entrez un nom de fichier avec l'extension `.cer`.
5. Créez une base de données de magasin de clés. Dans la boîte de dialogue **Nouveau**, procédez comme suit :
   a. Dans la liste **Key database type**, sélectionnez **CMS**, puis entrez un nom de fichier et un emplacement. A l'invite, entrez un mot de passe pour le nouveau fichier de clés.

      Remarque : Veillez à sélectionner **Stash the password to a file**.
   b. Si des certificats de signataire ont été extraits du fichier .pfx, procédez comme suit :
      1) Sélectionnez **Key Database Content** > **Signer Certificates**.
      2) Pour chaque certificat de signataire, cliquez sur **Ajouter** et ajoutez le fichier `.cer`.
   c. Sélectionnez **Key Database Content** > **Personal Certificates**, puis cliquez sur **Import**.
   d. Sélectionnez le type de fichier de clés **PKCS12**, et le nom et l'emplacement du fichier **.p12**. A l'invite du système, entrez le mot de passe.
   e. Sauvegardez le fichier de clés et quittez l'utilitaire de gestion de clés.
   f. Copiez les fichiers `.kdb` et `.sth` dans KT5Keystore sur la machine Response Time Monitoring.
   g. Placez les fichiers de base de données IBM Key Management (`.kdb`) et de stockage (`.sth`) dans un répertoire sûr, et assurez-vous que seul l'administrateur ou le `superutilisateur` (ou l'ID utilisateur qui a servi à installer l'agent Response Time Monitoring) peut les lire.

Configuration avancée de Packet Analyzer

Il existe un certain nombre d'options de configuration avancées pour Packet Analyzer.

Une fois que vous avez configuré Packet Analyzer, il existe certaines tâches de configuration avancées que vous pouvez effectuer pour affiner les performances et les fonctionnalités.

Utilisation des équilibreurs de charge :

Si vous utilisez des équilibreurs de charge dans votre environnement, il est nécessaire de les personnaliser.

Procédure

Si vous utilisez un équilibreur de charge, procédez comme suit :

1. Désactivez la réécriture des URL sur l'équilibreur de charge.
2. Installez un agent Response Time Monitoring sur chaque serveur Web que vous souhaitez surveiller. N'installez pas Response Time Monitoring sur l'équilibreur de charge.
3. Ajoutez le composant de surveillance JavaScript à votre application. Pour plus d'informations, voir «Ajout du composant de surveillance JavaScript à votre application», à la page 657.

Que faire ensuite

Si vous exécutez l'agent Response Time Monitoring derrière un équilibreur de charge, vous pouvez configurer ce dernier afin qu'il achemine l'adresse IP du client pour optimiser les performances de surveillance. Par exemple, reportez-vous à la procédure suivante :

1. Dans l'en-tête HTTP, définissez l'adresse IP du client dans la zone **X-Forwarded-For**.
2. Configurez l'agent Response Time Monitoring pour qu'il utilise l'en-tête d'adresse IP du client. Définissez l'en-tête d'adresse IP du client dans la zone **KFC_OVERRIDE_SOURCE_ADDR_HEADER**, dans l'un des fichiers suivants, en fonction de votre système d'exploitation :
   - AIX Linux `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`
   - Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`

   Par exemple :

   ```
   KFC_OVERRIDE_SOURCE_ADDR_HEADER=x-forwarded-for
   ```

   ou si vous utilisez WebSEAL :

   ```
   KFC_OVERRIDE_SOURCE_ADDR_HEADER=adresse_éloignée_iv
   ```

Configuration de la limite de surcharge de l'UC :

Si vous utilisez un environnement où les charges de transactions sont élevées, vous pouvez limiter les ressources de surveillance utilisées par l'agent Response Time Monitoring.

Pourquoi et quand exécuter cette tâche

Cette fonction limite l'utilisation de l'UC de l'agent Response Time Monitoring en surveillant et en signalant uniquement une partie du trafic Web à l'aide d'échantillons. La `limite de surcharge de l'UC` n'est pas configurée par défaut. Vous devez configurer la `limite de surcharge de l'UC` sur le serveur où l'agent est installé.

Procédure

Pour configurer la `limite de surcharge de l'UC`, procédez comme suit :

1. Ouvrez l'un des fichiers suivants en fonction de votre système d'exploitation :
   - AIX Linux `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`
   - Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`
2. Configurez les valeurs des paramètres suivants :

KFC_MAX_PROTOCOL_PACKETRATE
Taux de paquets maximal initial. Par exemple, si vous spécifiez **KFC_MAX_PROTOCOL_PACKETRATE=2000**, le taux de paquets maximal est de 2000 paquets par seconde. Ce taux varie de manière dynamique en fonction de la valeur du paramètre **KFC_CPUTHROTTLE_TARGET** et de la quantité d'UC actuellement utilisée.

KFC_CPUTHROTTLE_TARGET
Pourcentage de la quantité globale de ressources d'UC qui peut être utilisé par le processus `kfcmserver`. Par exemple, si vous spécifiez **KFC_CPUTHROTTLE_TARGET=10.0**, le processus `kfcmserver` peut utiliser jusqu'à 10 % des ressources d'UC globales.

Remarque : La valeur du paramètre **KFC_CPUTHROTTLE_TARGET** correspond au pourcentage de ressources d'UC globales disponible pour le processus `kfcmserver`. Par exemple, si vous disposez de 4 noyaux d'unités centrales et si **KFC_CPUTHROTTLE_TARGET** est défini sur 10, le moniteur de ressources de Windows mesure les ressources d'UC sur 400%. Par conséquent, le processus `kfcmserver` peut utiliser jusqu'à 40 % de la quantité totale de ressources d'UC disponibles (400 %).

Résultats

La `limite de surcharge de l'UC` est configurée pour l'agent Response Time Monitoring.

Personnalisation des valeurs de localisation Transaction utilisateur final

Vous pouvez personnaliser les localisations appliquées à des adresses IP ou à des plages d'adresses IP spécifiques dans les tableaux de bord Transaction utilisateur final pour votre environnement.

Avant de commencer

Utilisez l'onglet **Geolocation** sous **Configuration d'agent** pour personnaliser les valeurs de localisation.

Utilisez cette fonction pour définir la localisation des adresses IP affichées comme **inconnues** dans le tableau de bord. Ces adresses peuvent être des adresses internes, comme `192.168.x.x` ou `10.x.x.x`, ou des adresses IP externes qui ne sont pas résolues. Vous pouvez également utiliser cette fonction pour ignorer les localisations incorrectes des adresses IP. Par exemple, si vous savez que l'adresse IP `9.1.1.1` est située à Los Angeles mais qu'elle apparaît en tant qu'adresse située à San Francisco, ignorez la localisation et associez l'adresse `9.1.1.1` à Los Angeles.

Pourquoi et quand exécuter cette tâche

Personnalisez les valeurs de localisation dans les tableaux de bord Transaction utilisateur final en téléchargeant un fichier CSV contenant les valeurs dont vous avez besoin. Vous trouverez un exemple de fichier CSV dans l'onglet **Geolocation**.

Le fichier CSV doit inclure les valeurs ci-dessous comme en-tête. Les valeurs peuvent être de n'importe quel ordre et les entrées doivent respecter cet ordre.

```
IP_ADDRESS, COUNTRY, REGION, CITY
```

Par exemple,

```
IP_ADDRESS, COUNTRY, REGION, CITY
10.0.5.0/24, Australia, WA, Perth
10.1.0.6, Australia, VIC, Melbourne
```

Vous pouvez indiquer une adresse IPv4 unique ou définir une plage d'adresses. Si vous indiquez une plage, assurez-vous que vous utilisez une valeur valide comprise entre 1 et 32.

Procédure

Pour personnaliser les valeurs de localisation affichées dans les tableaux de bord Transaction utilisateur final, effectuez les opérations suivantes dans le tableau de bord d'Application Performance.

1. Configurez votre fichier ou vos fichiers CSV ; les adresses IP doivent correspondre aux localisations.
2. Téléchargez le fichier CSV.
   a. Accédez à **Configuration d'agent** > **Geolocation**.
   b. Cliquez sur **Upload CSV**, sélectionnez les fichiers à télécharger, puis cliquez sur **Ouvrir**.
      - Vérifiez que le fichier CSV répertorie les plages d'adresses IP générales en premier, suivies des adresses IP plus spécifiques.
      - Téléchargez plusieurs fichiers si nécessaire.
      - Si les valeurs d'un fichier chevauchent celles d'un autre fichier, les valeurs du fichier le plus récent prévalent sur celles de l'autre fichier.
3. Développez **Upload Results** à la recherche d'éventuelles erreurs. Recherchez les problèmes suivants :
   - Substitutions
   - Adresses IP non valides
   - Lignes non valides
   - Valeurs comportant plus de 250 caractères

Résultats

Patientez quelques minutes et affichez vos valeurs personnalisées dans les tableaux de bord Transaction utilisateur final.

Que faire ensuite

Vous pouvez supprimer des valeurs personnalisées si nécessaire. Effectuez l'une des étapes suivantes :

- Pour supprimer certaines valeurs personnalisées, sélectionnez les adresses IP à supprimer, cliquez sur **Clear Selected Entries**, puis sur **OK** pour confirmer la suppression.
- Pour supprimer toutes les valeurs personnalisées, cliquez sur **Clear All Entries**, puis sur **OK** pour confirmer la suppression.

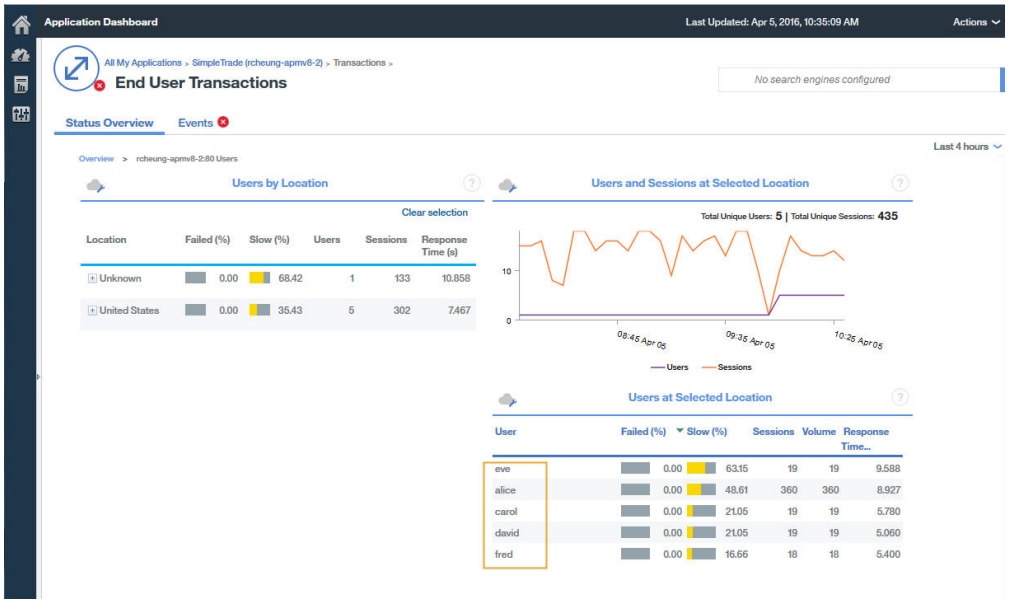
Suivi des applications Web supplémentaires

Pour suivre des applications Web en plus de celles déjà suivies par défaut, vous devez identifier et configurer les méthodes de suivi des utilisateurs et des sessions.

Avant de commencer

Si votre application n'est pas prise en charge par défaut, les tableaux de bord ne contiennent aucun détail d'utilisateur et de session ; le nom d'utilisateur s'affiche comme `anonymous` ou `unknown`, et aucune information de session n'est disponible.

Si les méthodes de suivi sont correctement configurées, l'ID utilisateur est extrait puis listé dans le tableau de bord **Transactions utilisateur final** > **User Summary** > **Utilisateurs à l'emplacement sélectionné**.



Dans IBM Performance Management (On Premises) v8.1.2 et versions antérieures, les ID utilisateur extraits sont listés dans **Utilisateurs authentifiés** dans le panneau de navigation.

Pourquoi et quand exécuter cette tâche

Dans IBM Application Performance Management V8.1.4 et versions ultérieures, vous pouvez utiliser la page **Configuration d'agent** > **Temps de réponse** pour ajouter les applications que vous souhaitez suivre au moyen de l'Analyseur de paquets ou du module IBM HTTP Server Response Time. Les valeurs définies sur cette page prévalent sur celles du fichier `WRT_Defaults.xml`.

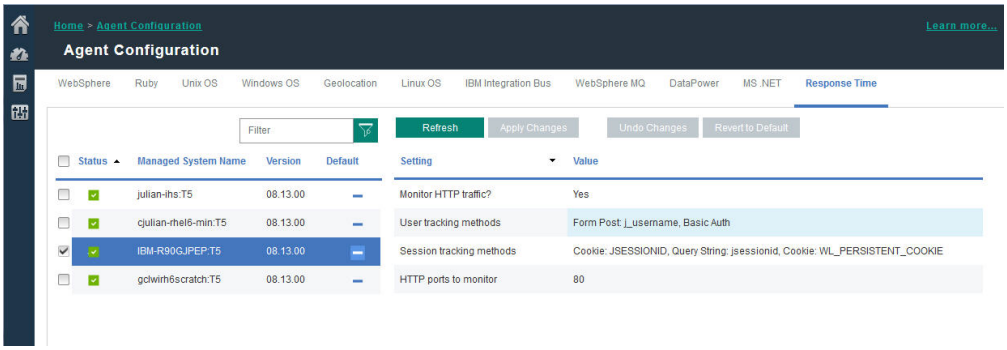
Pour suivre des applications supplémentaires, vous devez d'abord identifier les méthodes et valeurs des ID utilisateur et session pour l'application que vous souhaitez suivre. Par exemple :

1. Ouvrez l'outil de développement de votre navigateur de sorte à afficher les demandes associées à l'application que vous souhaitez suivre.
2. Sélectionnez la dernière demande dans le journal de réseau du navigateur afin d'identifier facilement votre demande test.
3. Créez une demande test à l'aide de paramètres reconnaissables. Par exemple, connectez-vous à votre site Web en tant qu'`utilisateur test`.
4. Sélectionnez la demande test et vérifiez les `en-têtes`.
5. Identifiez l'ID session dans le journal des demandes. L'ID session est généralement spécifié dans le contenu `cookie`, `POST`, `en-tête de demande/réponse` ou `chaîne de requête`. Si le `cookie` est déjà défini dans le profil par défaut, vous n'avez pas besoin de l'ajouter à l'étape 2.
6. Identifiez l'ID utilisateur dans le journal des demandes. L'ID utilisateur peut être spécifié dans le contenu `cookie`, `en-tête de demande`, `POST` ou `chaîne de requête`. Par exemple, recherchez `utilisateur test` pour obtenir la valeur de l'ID utilisateur.

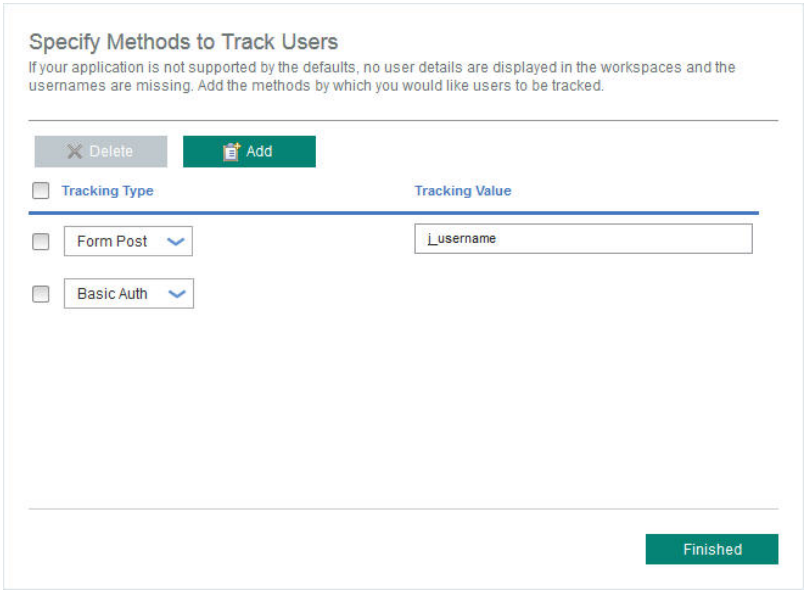
Procédure

Une fois les méthodes et valeurs de suivi des utilisateurs et des sessions utilisées dans votre application identifiées, procédez comme suit :

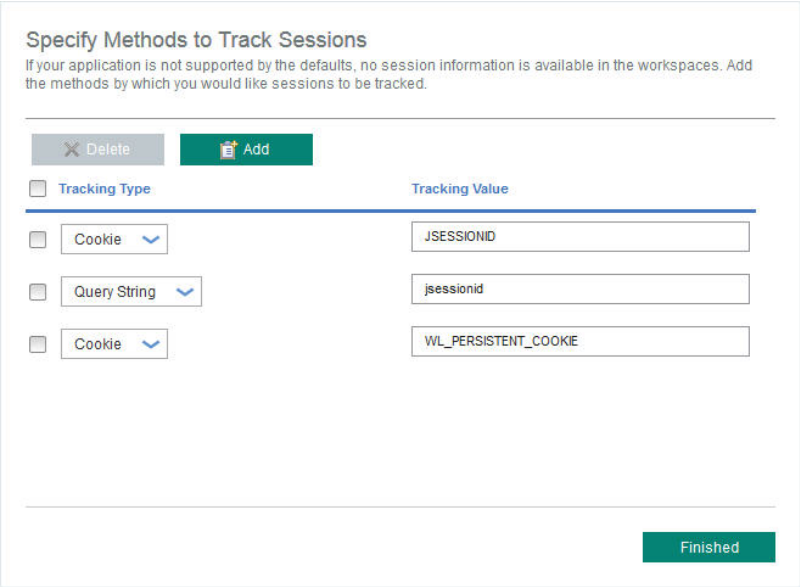
1. Accédez à la page de configuration **Configuration d'agent** > **Temps de réponse**.



2. Sélectionnez le système géré que vous souhaitez mettre à jour.
3. Si nécessaire, mettez à jour les méthodes de suivi des utilisateurs :
   a. Cliquez sur la valeur dans la zone **Méthodes de suivi des utilisateurs**.



   b. Dans la fenêtre **Spécifiez les méthodes de suivi des utilisateurs**, cliquez sur **Ajouter**.
   c. Dans la liste **Type de suivi**, sélectionnez le type de suivi. Par exemple, `En-tête`.
   d. Dans la zone **Valeur de suivi**, indiquez une valeur. Par exemple, `nom d'utilisateur`.
   e. Cliquez sur **Terminé**.
4. Si nécessaire, mettez à jour les méthodes de suivi des sessions :
   a. Cliquez sur la valeur dans la zone **Méthodes de suivi des sessions**.



b. Dans la fenêtre **Spécifiez les méthodes de suivi des sessions**, cliquez sur **Ajouter**.
c. Dans la liste **Type de suivi**, sélectionnez le type de suivi. Par exemple, `Cookie`.
d. Dans la zone **Valeur de suivi**, indiquez une valeur. Par exemple, `WL_PERSISTENT_COOKIE`.
e. Cliquez sur **Terminé**.

5. Sur la page Configuration d'agent, cliquez sur **Appliquer les modifications**.

Résultats

Les applications auxquelles les nouvelles méthodes de suivi indiquées sont appliquées figurent dans le Tableau de bord des applications.

Que faire ensuite

Vérifiez que les ID utilisateur et informations de session associés à l'application figurent dans le Tableau de bord des applications.

Spécification d'un nom de système géré unique pour l'Agent de surveillance des temps de réponse

Le nom d'instance de l'Agent de surveillance des temps de réponse affiché sur la console du Cloud APM est également appelé nom de système géré (MSN). Vous pouvez utiliser le paramètre de configuration d'agent afin d'indiquer un MSN unique pour chaque instance d'agent.

Pourquoi et quand exécuter cette tâche

Le nom de système géré de l'Agent de surveillance des temps de réponse est au format suivant :
nom_instance`:`*nom_hôte*`:T5`

`T5` est le code produit de l'Agent de surveillance des temps de réponse.

Procédure

1. Arrêtez toutes les instances d'agent existantes. S'il n'en existe aucune, passez à l'étape suivante. Pour plus d'informations sur l'arrêt des instances d'agent, voir «Utilisation des commandes de l'agent», à la page 213.

2. Linux AIX Modifiez **CTIRA_SUBSYSTEM_ID** dans le fichier `runagent`. En général, toutes les instances d'agent sur un ordinateur utilisent la même valeur de nom d'hôte.
   a. Effectuez une copie de sauvegarde du fichier : Linux AIX
      rép_install`/`*plateforme*`/t5/bin/runagent`
   b. Modifiez le fichier. Ajoutez *nouveau_nom_instance* sur les systèmes Linux ou AIX.
      Linux AIX
      CTIRA_SUBSYSTEM_ID=*nouvel_id_sous_système*
3. Démarrez les instances existantes de l'agent.
4. Lancez la console Cloud APM. Modifiez vos applications en supprimant les instances d'agent sous les anciens MSN et en ajoutant les nouvelles instances d'agent.

Configuration de la surveillance de Ruby

Vous pouvez surveiller les applications Ruby sur site et IBM Cloud. Pour surveiller les applications Ruby sur site, configurez l'Agent Ruby. Pour surveiller les applications Ruby IBM Cloud, configurez le collecteur de données Ruby.

Pourquoi et quand exécuter cette tâche

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'Agent Ruby et le collecteur de données Ruby. Effectuez les étapes de configuration en fonction de vos besoins.

Procédure

- Pour surveiller les applications Ruby sur site, effectuez les étapes suivantes pour configurer l'Agent Ruby :
  1. Configurez des instances d'agent pour surveiller les applications Ruby. Voir Configuration de l'Agent Ruby pour surveiller les applications Ruby.
  2. Installez le collecteur de données pour surveiller les données à afficher dans la console Cloud APM. Voir Installation du collecteur de données.
  3. Facultatif : Si vous êtes un utilisateur Cloud APM, Advanced, vous pouvez procéder comme suit en fonction de vos besoins :
     - Pour configurer le collecteur de données afin qu'il collecte des données de diagnostic, voir Configuration du collecteur de données de diagnostic.
     - Pour activer la trace de méthode pour les demandes et ajuster la longueur du paramètre de chemin d'accès au fichier qui s'affiche dans le widget Trace de pile des demandes, voir Activation du suivi des méthodes et ajustement de l'affichage de chemin.
     - Pour augmenter la taille de segment de mémoire de JVM afin d'éviter l'erreur `out of memory`, voir Augmentation de la taille de segment de mémoire de JVM.
     - Pour désactiver les diagnostics, voir Désactivation ou activation des données de diagnostic pour les applications Ruby.
- Pour surveiller les applications Ruby IBM Cloud, effectuez les tâches suivantes pour configurer le collecteur de données Ruby :
  1. Configurez le collecteur de données Ruby pour les applications IBM Cloud. Pour plus d'informations, voir «Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 677.
  2. Facultatif : Pour modifier le comportement du collecteur de données Ruby, voir «Personnalisation du collecteur de données Ruby pour les applications IBM Cloud», à la page 678.

Configuration de l'Agent Ruby

Pour que l'Agent Ruby surveille vos applications, indiquez la durée d'exécution de Ruby. Utilisez ainsi cette durée d'exécution pour regrouper les données issues des applications Ruby et configurer l'agent.

Avant de commencer

Identifiez le serveur que vous allez utiliser pour démarrer les applications Ruby ainsi que le répertoire bin qualifié contenant l'exécutable Ruby ou Rake utilisé par l'agent :

1. Pour déterminer le serveur d'applications que vous allez utiliser, exécutez la commande suivante :

   ```
   ps -ef | grep ruby
   ```

   Le nom du serveur utilisé pour démarrer votre application s'affiche. Les noms de serveur possibles sont répertoriés comme suit :

   - `Passenger`
   - `Unicorn`
   - `Puma`
   - `Thin`

   Si le résultat de la commande n'indique aucun des noms de serveur mentionnés ci-dessus, le serveur que vous utilisez pour démarrer l'application sera peut-être WEBrick.

   Important : Si vous utilisez plusieurs serveurs Web pour démarrer vos applications Ruby, vous devez créer une instance d'agent pour chaque serveur Web d'application : une instance pour PUMA et une pour Unicorn par exemple.
2. Pour déterminer le répertoire bin qualifié contenant l'exécutable Ruby ou Rake utilisé par l'Agent Ruby, exécutez la commande suivante :

   ```
   which ruby
   ```

Pourquoi et quand exécuter cette tâche

Vous pouvez répéter cette tâche pour configurer plusieurs instances d'agent en fonction de vos besoins.

Procédure

1. Pour configurer l'agent, exécutez la commande suivante :
   rép_install`/bin/ruby-agent.sh config` *nom_instance*
   où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

   Important : N'indiquez pas de nom d'instance long. La longueur totale de votre nom d'hôte et du nom d'instance d'agent ne doit pas dépasser 28 caractères. Si la longueur dépasse la limite, le nom de système géré est tronqué et le code produit de l'Agent Ruby ne s'affiche pas correctement.

   Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*`:`*nom_hôte*`:`*pc* par exemple, où *pc* est le code produit à deux caractères de l'agent. Par exemple, si vous indiquez `Ruby2` comme nom d'instance, votre nom de système géré est `Ruby2:hostname:KM`, où *KM* correspond au code produit à deux caractères de l'Agent Ruby.
2. A l'invite `Edit 'Monitoring Agent for Ruby' settings`, entrez `1` pour continuer.
3. A l'invite `Fully Qualified Rubies Bin Directory`, indiquez le répertoire bin. Par exemple, si vous utilisez Ruby Version Manager (RVM), entrez `/usr/local/rvm/rubies/ruby-2.0.0-p247/bin`.
4. A l'invite `Auto Detect Ruby Applications Flag`, entrez `Y` pour continuer. L'agent reçoit les données envoyées par le collecteur de données de l'agent.
5. A l'invite `Application Server Process name`, appuyez sur Entrée pour accepter la valeur par défaut de `ruby`, ou spécifiez la valeur du serveur que vous utilisez en vous référant à la liste suivante :

- Pour les serveurs WEBrick, acceptez la valeur par défaut ou spécifiez `ruby` ; si le composant Rails est installé par Ruby Stack, spécifiez `.ruby.bin`.
- Pour les serveurs Passenger, spécifiez `passenger`.
- Pour les serveurs Unicorn, spécifiez `unicorn`.
- Pour les serveurs Puma, spécifiez `puma`.
- Pour les serveurs Thin, si les applications sont démarrées en exécutant la commande `thin start`, acceptez la valeur par défaut pour utiliser `ruby` ; si les applications sont démarrées en utilisant la commande `thin start -d`, spécifiez `thin` ; si le composant Rails est installé par Ruby Stack et que les applications sont démarrées en exécutant la commande `thin start`, spécifiez `.ruby.bin`.

6. A l'invite `Socket Data Source`, appuyez sur Entrée pour accepter la valeur par défaut `0` permettant d'utiliser le port temporaire.
7. A l'invite `Edit 'Application' settings`, entrez `5` pour quitter.
8. Pour démarrer l'agent, exécutez la commande suivante :
   rép_install`/bin/ruby-agent.sh start` *nom_instance*

Que faire ensuite

Installez le collecteur de données pour que l'Agent Ruby fonctionne correctement et pour que les données s'affichent dans l'interface utilisateur de Cloud APM. Pour plus d'informations, voir Installation du collecteur de données

Installation du collecteur de données

Vous devez installer le collecteur de données pour que l'agent fonctionne correctement. Après avoir installé le collecteur de données, les données de surveillance s'affichent dans le Tableau de bord d'Application Performance.

Avant de commencer

Si vous avez installé une application Ruby on Rails sur un système Linux en utilisant un compte utilisateur non superutilisateur et que vous prévoyez de collecter des données de diagnostic, l'utilisateur non superutilisateur doit avoir accès au répertoire de base du collecteur de données de diagnostic. Vérifiez que l'utilisateur non superutilisateur dispose d'un accès en lecture et en écriture au répertoire *rép_install*`/install-images/kkm`, où *rép_install* correspond au répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`. Entrez si nécessaire les droits d'accès en lecture et en écriture à l'aide de la commande `chmod 777`.

Procédure

1. Arrêtez votre application Ruby on Rails.
2. Facultatif : Si vous mettez à niveau le collecteur de données Ruby to a new version, vers une nouvelle version, vous devez au préalable désinstaller l'ancienne version du collecteur de données en exécutant la commande suivante :

   ```
   gem uninstall stacktracer
   ```

3. Installez le collecteur de données de diagnostic. Entrez `gem install --local` *rép_install*`/lx8266/km/bin/stacktracer-`*version*`.gem`, où *version* est le numéro de version et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le numéro de version du fichier `stacktracer-`*version*`.gem` dans le répertoire d'installation indique le numéro de version dont vous avez besoin pour entrer ici. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

   Important : Installez le collecteur de données avec le même ID utilisateur que vous avez utilisé pour installer et exécuter l'application Ruby on Rails.
4. Accédez au répertoire principal de votre application, ouvrez le fichier `Gemfile` et ajoutez la ligne suivante à la fin du fichier : `gem 'stacktracer', '`*version*`'`
   où *version* est le numéro de version du collecteur de données. Le numéro de version se trouve dans le

nom du fichier `stacktracer-version.gem` qui se trouve dans *rép_install* de l'Agent Ruby. Par exemple, si vous installez le collecteur de données Ruby Version 1.0 Fix Pack 8, le fichier `stacktracer-01.00.08.00.gem` se trouve dans le répertoire d'installation de l'agent. Ensuite, ajoutez la ligne `gem 'stacktracer', '01.00.08.00'` à votre application pour installer le collecteur de données.

Remarque : S'il n'existe qu'une seule version de `stacktracer` dans l'environnement, ajoutez la ligne `gem 'stacktracer'` à la fin du fichier. Ne spécifiez pas le numéro de version dans la ligne.

5. Dans le répertoire de base de votre application, entrez `bundle install`.
6. Redémarrez l'application Ruby on Rails.

Résultats

Le collecteur des données est installé et configuré, et l'application Ruby on Rails est démarrée.

Que faire ensuite

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 989. Sélectionnez **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**, puis explorez en aval les tableaux de bord de diagnostics et de surveillance des ressources des applications Ruby pour observer les applications Ruby on Rails du récapitulatif des statuts jusqu'aux instances de demande individuelles.
- Pour afficher et modifier les paramètres du collecteur des données diagnostics, passez à la rubrique suivante, «Configuration du collecteur de données de diagnostic».
- Pour afficher les données de trace de méthode pour les demandes dans l'interface utilisateur de Cloud APM, voir Activation du suivi des méthodes et ajustement de l'affichage de chemin.
- Lorsque la trace de méthode est activée ou que le nombre de demandes de données est élevé, vous risquez de recevoir des erreurs `out of memory`. Vous pouvez augmenter la taille de segment de mémoire de JVM afin d'éviter ces erreurs. Voir Augmentation de la taille de segment de mémoire de JVM.
- Vous pouvez désactiver ou activer à tout moment la collecte des données de diagnostic pour une ou plusieurs applications Ruby on Rails gérées via la console Cloud APM. Voir «Désactivation ou activation des données de diagnostic pour les applications Ruby», à la page 676. Cette fonction n'est pas disponible pour la surveillance des ressources.

Configuration du collecteur de données de diagnostic

Si vous êtes un utilisateur de Cloud APM, Advanced, vous pouvez continuer à configurer le collecteur de données pour les données de diagnostic. La collecte des données de diagnostic est désactivée par défaut dans le fichier de configuration du collecteur de données.

Avant de commencer

Vous devez avoir installé le collecteur de données de diagnostics et configuré la prise en charge de la collecte des données de diagnostic, comme indiqué dans «Installation du collecteur de données», à la page 671.

Pourquoi et quand exécuter cette tâche

Le fichier de configuration `instrumenter_settings.rb` apparaît une fois que l'agent a enregistré l'existence d'un application Ruby on Rails en configurant correctement le fichier `Gemfile`. Ce fichier de configuration peut être modifié pendant que l'agent Ruby est actif, et les modifications sont appliquées automatiquement. Vous pouvez également appliquer les modifications à toutes les applications Ruby on Rails surveillées, ce qui implique d'arrêter les applications pendant que vous modifiez le fichier de configuration.

Procédure

- Pour modifier les paramètres du collecteur de données pour une application spécifique en cours d'exécution :
  1. Accédez au répertoire *rép_install*/install-images/kkm/dchome/*appClassName*/config, où *appClassName* est le nom de classe d'application Ruby, et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est /opt/ibm/apm/agent.
  2. Ouvrez instrumenter_settings.rb dans un éditeur de texte.
  3. Modifiez les paramètres du collecteur de données :

     :instrumentation_enabled
     Pour activer le support de la collecte des données de diagnostic, définissez :instrumentation_enabled => true.

     Pour désactiver le support de la collecte des données de diagnostic, définissez :instrumentation_enabled => false.

     :sample_frequency
     Pour modifier la fréquence d'échantillonnage de demandes, entrez le nombre de demandes entre les échantillonnages.

     Le collecteur de données ne rassemble les données de diagnostic que pour les demandes échantillonnées. Si vous définissez la propriété :sample_frequency => 10, par exemple, les données sont collectées pour 1 demande sur 10.

     :max_methods_to_instrument
     Pour désactiver ou activer la collecte des données de trace des méthodes et limiter le nombre de méthodes à suivre, définissez la valeur zéro ou entrez le nombre maximal de méthodes à suivre.

     Pour désactiver la collecte des données de trace des méthodes, définissez :max_methods_to_instrument => 0.

     Pour l'activer, définissez :max_methods_to_instrument => 10000. Cette valeur peut être plus élevée, mais pas trop afin d'éviter une baisse des performances. Lorsque les données des méthodes sont collectées, les appels aux méthodes sont inclus dans le widget Trace des méthodes du tableau de bord Traces des demandes, ce qui permet d'afficher toutes les instances de demande et leurs demandes imbriquées.

     :min_wallclock_to_include_in_trace
     Pour modifier le seuil qui détermine si la demande ou la méthode doit être tracée, définissez le temps minimum de réponse. Si vous définissez :min_wallclock_to_include_in_trace => 0.001, par exemple, seules les demandes et les méthodes dont les temps de réponse dépassent 1 milliseconde sont suivis.

     A faire : Dans le tableau de bord des diagnostics Trace des demandes, vous pouvez explorer en aval vers une instance de demande depuis le widget de groupe Trace de pile de demande. Les totaux des temps de réponse de l'instance peuvent être incorrects du fait des filtres définis pour :min_wallclock_to_include_in_trace et :min_wallclock_to_include_stacks, qui peuvent exclure des données.

     :min_wallclock_to_include_stacks
     Pour modifier le seuil qui détermine si les informations de trace de pile doivent être collectées pour une demande ou une méthode, définissez le temps de réponse minimum.

     Si vous définissez :min_wallclock_to_include_stacks => 0.1, par exemple, les informations de trace de pile sont collectées pour toutes les demandes et méthodes dont le temps de réponse est supérieur à 100 millisecondes.

     :include_subclasses_of_these_modules
     Le tableau de bord des diagnostics Trace des demandes permet d'identifier la séquence des

appels aux demandes imbriquées et aux méthodes d'une instance de demande. Le collecteur des données filtre à l'avance les méthodes des classes qui ne sont pas incluses dans la liste de filtres. Si des opérations à suivre ne sont pas incluses dans les traces de pile des méthodes, vous pouvez les ajouter ici.

Pour définir les méthodes à suivre, ajoutez leurs noms de classe.

Supposons que vous vouliez tracer les API Moped dans le type de code Ruby suivant :

```
session = Moped::Session.new(['ip:27017'])
session.use(:HR)
session[:profiles].insert({......})
session[:profiles].find({...}).remove
```

Ajoutez les noms de module de ces API Moped à la propriété :

```
:include_subclasses_of_these_modules => {"
ActionController" => true,
                     "ERB" => true,
                     "erb" => true,
                     "Arel" => true,
                     "Mongoid" => true,
                     "Moped" => true
                    },
```

Restriction : Les traces de méthode n'incluent pas les méthodes de classe et les méthodes privées (méthodes définies dans une classe, qui ont des spécificateurs d'accès «privé» implicite ou explicite).

:include_sql_text
Pour collecter les données de contexte pour les méthodes, affectez à cette propriété la valeur `true`.

:num_samples_per_file
Pour modifier le nombre maximal de demandes suivies à stocker dans chaque fichier, entrez une valeur, telle que `:num_samples_per_file => 1000`. Lorsque la limite définie ici est atteinte, un nouveau fichier est créé.

Envisagez d'affecter au paramètre `:num_samples_per_file` une valeur inférieure si vous ajustez la configuration de manière à ce que davantage de données soient collectées. Par exemple, la définition de `:include_subclasses_of_these_modules` pour effectuer le suivi d'un nombre plus élevé de classes et de méthodes peut augmenter la collecte de données. L'affectation d'une valeur inférieure à l'une des propriétés suivantes peut également augmenter la collecte de données : `:sample_frequency`, `:min_wallclock_to_include_in_trace` et `:min_wallclock_to_include_stacks`.

:verbose_request_instrumentation
:verbose_class_instrumentation
:verbose_method_instrumentation
Pour augmenter le niveau de consignation du collecteur des données de diagnostic, affectez à ces propriétés la valeur `true`.

Conseil : Si les opérations que vous voulez tracer ne sont pas incluses dans les traces de pile des méthodes, définissez `:verbose_class_instrumentation => true` et vérifiez le journal pour déterminer si la classe à suivre est instrumentée. Si tel n'est pas le cas, ajoutez le nom de classe du nom du module de la classe à la propriété `:include_subclasses_of_these_modules` property.

4. Si vous avez modifié des propriétés, redémarrez l'application Ruby on Rails correspondante pour appliquer les modifications :

```
:include_subclasses_of_these_modules
:max_methods_to_instrument
```

Le redémarrage est nécessaire, car ces propriétés sont utilisées uniquement lorsqu'une application est lancée pour déterminer la classe ou la méthode que le collecteur des données Ruby doit instrumenter.

- Pour modifier les paramètres du collecteur de données de toutes les applications, procédez comme suit :
  1. Arrêtez les applications Ruby on Rails en cours d'exécution.
  2. Retirez le fichier `instrumer_settings.rb` du répertoire *rép_install*`/install-images/kkm/dchome/`*nom_application*`/config`.
  3. Modifiez les paramètres du collecteur de données dans le fichier *rép_Gem*`/gems/stacktracer-`*version*`/config/instrumenter_settings_template.rb` où *version* correspond au numéro de version, comme 01.00.05.00, et *rép_Gem* au répertoire d'installation de `stacktracer-version.gem`, tel que `/usr/local/rvm/gems/ruby-2.1.4/`. Pour plus d'informations, voir l'étape 3, à la page 673 dans la procédure de modification des paramètres du collecteur de données pour une application spécifique.
  4. Redémarrez les applications Ruby on Rails en cours d'exécution.

Résultats

La configuration du collecteur de données de diagnostic a été modifiée pour l'application en cours d'exécution que vous avez spécifiée ou pour toutes les applications.

Activation du suivi des méthodes et ajustement de l'affichage de chemin

IBM Cloud Application Performance Management, Advanced Private avec données de diagnostic permet aux utilisateurs de disposer d'un tableau de bord Traces de demande. Si les données des méthodes sont collectées, les appels aux méthodes sont affichés.

Le widget Trace des méthodes affiche les instances de demande et leurs demandes imbriquées. Vous pouvez activer la trace des méthodes pour inclure les appels aux méthodes dans les demandes imbriquées. Vous pouvez également ajuster la configuration du widget Trace de pile de demande pour afficher plus de 50 caractères par défaut pour chaque chemin de fichier.

Pourquoi et quand exécuter cette tâche

Le suivi des méthodes est activé par défaut. Exécutez la première procédure pour activer le suivi des méthodes afin de l'afficher dans le tableau Traces des demandes. Vous pouvez activer le suivi des méthodes en changeant un paramètre dans le fichier de configuration.

Exécutez la seconde procédure pour ajuster le nombre de caractères indiqué dans le chemin de fichier dans le widget Trace de pile de demande.

Procédure

- Pour activer le suivi des méthodes, modifiez les paramètres `instrumenter_settings.rb` :
  1. Recherchez le fichier `instrumenter_settings.rb` dans l'installation de l'Agent Ruby, par exemple, *rép_install*`/install-images/kkm/dchome/`*appClassName*`/config` où *appClassName* est le nom de classe d'application Ruby, et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
  2. Ouvrez `instrumenter_settings.rb` dans un éditeur de texte.
  3. Affectez la valeur 10000 à la propriété suivante.

     ```
     max_method_to_instrument
     ```

     Cette valeur peut être plus élevée, mais pas trop afin d'éviter une baisse des performances. (Voir aussi «Augmentation de la taille de segment de mémoire de JVM», à la page 676.)
  4. Redémarrez les applications Ruby on Rails pour lancer la collecte des données des méthodes.

Pour plus d'informations sur toutes les propriétés `instrumenter_settings.rb`, voir «Configuration du collecteur de données de diagnostic», à la page 672.

- Pour ajuster la taille d'affichage du chemin de fichier dans le widget Trace de pile de demande, modifiez le fichier `dfe.properties` :
  1. Recherchez le fichier `dfe.properties` dans l'installation de l'Agent Ruby, par exemple, *rép_install*`/lx8266/km/bin/dfe.properties`
     où *rép_install* correspond au répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
  2. Ouvrez `dfe.properties` dans un éditeur de texte.
  3. Changez la taille maximum du chemin de fichier à afficher dans chaque élément de la trace de pile en ajustant la valeur de la propriété suivante :

     ```
     dfe.stacktrace.filepath.maxsize
     ```
  4. Redémarrez l'Agent Ruby.

Augmentation de la taille de segment de mémoire de JVM

Lorsque la trace des méthodes est activée pour le tableau de bord Traces des demandes des diagnostics Ruby, ou que les demandes sont très grandes, vous pouvez augmenter la taille du segment de mémoire pour éviter les erreurs de manque de mémoire.

Pourquoi et quand exécuter cette tâche

L'Agent Ruby est un agent Java et la taille de segment de mémoire de JVM par défaut est de 384 Mo. Pour augmenter la taille de segment et réduire ainsi les risques de saturation de la mémoire, procédez comme suit. L'erreur de saturation de mémoire peut se produire lorsque les demandes de données de grande taille sont fréquentes et que la trace de méthode est activée.

Procédure

1. Recherchez le paramètre de taille de segment JVM dans le répertoire d'installation de l'Agent Ruby, comme *rép_install*`/lx8266/km/bin/runDeepDiveClient.sh`
   Où *rép_install* correspond au répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`. La valeur par défaut est `-Xmx384m`.
2. Augmentez cette valeur jusqu'à 1024 Mo par exemple, comme dans `-Xmx1024m` :

   ```
   export JAVA_OPT="-Djlog.common.dir=$CANDLEHOME/logs -DCONFIG_DIR=$DC_RUNTIME_DIR
   -Dkqe.cache.interval=60 -Xmx1024m -Dkqe.timespan=900 -Djlog.propertyFileDir.CYN=$CANDLEHOME/
   $ITM_BINARCH/$PRODUCT_CODE/bin"
   ```
3. Redémarrez l'Agent Ruby.

Désactivation ou activation des données de diagnostic pour les applications Ruby

Si vous disposez d'IBM Cloud Application Performance Management, Advanced Private, vous pouvez utiliser la page Configuration d'agent dans la console Cloud APM pour désactiver ou activer la collecte des données de diagnostic à tout moment pour un ou plusieurs systèmes gérés.

Avant de commencer

- Vous devez disposer de l'outil Cloud APM, Advanced Private dans votre environnement.

  Remarque : Cette fonction n'est pas disponible pour IBM Monitoring.
- Vous devez installer et configurer l'Monitoring Agent for Ruby sur une machine virtuelle, comme indiqué dans «Installation d'agents», à la page 167 sur des systèmes AIX ou «Installation d'agents», à la page 175 sur des systèmes Linux et dans «Configuration de la surveillance de Ruby», à la page 669.
- Vous devez installer le collecteur de données des diagnostic et configurer la prise en charge de la collecte des données de diagnostic, comme indiqué dans «Installation du collecteur de données», à la page 671.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez configuré la prise en charge des données de diagnostic dans la configuration du collecteur de données, la collecte des données de diagnostic est désactivée par défaut pour chaque système géré. Pour afficher des données dans les tableaux de bord de diagnostic, vous devez activer la collecte de diagnostic pour chaque système géré que vous surveillez.

Exécutez les étapes suivantes pour activer et désactiver la collecte de données de diagnostic pour chaque système géré :

Procédure

1. Dans la barre de navigation, sélectionnez **Configuration du système -> Configuration d'agent**. La page Configuration d'agent s'affiche.
2. Cliquez sur l'onglet **Ruby**.
3. Cochez la case des systèmes gérés pour lesquels vous voulez désactiver ou activer la collecte des diagnostics.
4. Dans la liste **Actions**, sélectionnez l'une des options suivantes pour désactiver ou activer la collecte des diagnostics des systèmes gérés sélectionnés :
   - Sélectionnez **Désactiver la collecte des données**. Le statut indiqué dans la colonne Collecte de données activée est mis à jour et devient Non pour chacun des systèmes gérés sélectionnés.
   - Sélectionnez **Activer la collecte des données**. Le statut indiqué dans la colonne Collecte de données activée est mis à jour et devient Oui pour chacun des systèmes gérés sélectionnés.

Résultats

Vous avez configuré la collecte des données de diagnostic pour chacun des systèmes gérés sélectionnés.

Configuration du collecteur de données Ruby pour les applications IBM Cloud

Pour collecter des informations concernant les applications Ruby sur IBM Cloud, vous devez configurer le collecteur de données Ruby.

Avant de commencer

1. Téléchargez le package du collecteur de données à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
2. Configurez le package du collecteur de données en exécutant les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `ruby_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
2. Procédez à l'extraction des fichiers dans `ruby_datacollector_8.1.4.0.tgz` en exécutant la commande suivante :

   ```
   tar -zxf ruby_datacollector_8.1.4.0.tgz
   ```

   Vous obtenez un dossier `ibm_ruby_dc`.
3. Copiez l'intégralité du dossier `etc` dans `ibm_ruby_dc` dans le dossier principal de votre application Ruby en exécutant la commande suivante :

   ```
   cp –r répertoire du dossier etc  répertoire de base de votre application Ruby
   ```

La commande suivante extrait le collecteur de données dans le répertoire /opt/ibm/ccm/ibm_ruby_dc/etc et le répertoire de base de votre application Ruby est /root/ruby_app/ :

```
cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
```

4. Ajoutez la section suivante au fichier Gemfile dans le dossier de base de votre application Ruby :

```
gem 'logger',  '>= 1.2.8'
source 'https://maagemserver.ng.bluemix.net/' do
  gem 'ibm_resource_monitor'
  gem 'stacktracer'
end
```

5. Exécutez la commande bundle lock pour régénérer le fichier Gemfile.lock.
6. A partir du répertoire qui contient le fichier manifest.yml de votre application Ruby, exécutez la commande suivante :

```
cf push
```

Conseil : Pour un fichier manifest.yml exemple, voir «Exemple de fichier manifest.yml», à la page 237.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez vérifier que les données de surveillance de votre application IBM Cloud s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Personnalisation du collecteur de données Ruby pour les applications IBM Cloud

Vous pouvez ajouter des variables d'environnement dans l'interface utilisateur (UI) IBM Cloud pour personnaliser la surveillance de votre application IBM Cloud. Utilisez les informations suivantes pour ajouter des variables en fonction de vos besoins.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Ruby

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance Ruby sur IBM Cloud.

Tableau 161. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Ruby sur IBM Cloud

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https://<*IP ou nom d'hôte du serveur*>:443 • http://<*IP ou nom d'hôte du serveur*>:80	L'URL de la passerelle de serveur sur site cible.

Tableau 161. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Ruby sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
APM_KEYFILE_PSWD	Facultative	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n <mot de passe du fichier de clés> | base64` pour chiffrer votre mot de passe. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	http://<*serveur http hébergé*>:<*port*>/keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous configurez la passerelle pour utiliser HTTPS.
kkm_instrumentation_enabled	Facultative	• true • false	Active ou désactive la collecte des données de diagnostic. true : si vous définissez la valeur sur `true`, les données de diagnostic sont collectées. false : si vous définissez la valeur sur `false`, les données de diagnostic ne sont pas collectées. La valeur par défaut est `true`.
kkm_max_methods_to_instrument	Facultative	Nombre maximal de méthodes tracées	Nombre maximal de méthodes tracées. Vous pouvez désactiver la trace de méthode en définissant la valeur sur `0`. Par défaut, la valeur est `10000` et la trace de méthode est activée. **Remarque :** Il est recommandé de ne pas définir une valeur supérieure à 10000. Une valeur très supérieure à 10000 peut altérer l'efficacité de l'exécution de l'application.
kkm_sample_frequency	Facultative	Fréquence des demandes par échantillonnage	Le nombre de demandes à partir duquel une demande d'échantillon est effectuée, par exemple, si vous définissez la valeur sur `10`, les données de surveillance sont collectées pour une demande sur 10. La valeur par défaut est `10`.

Tableau 161. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Ruby sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
kkm_min_wallclock_to_include_in_trace	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en secondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. Si vous définissez cette variable sur 0,001, par exemple, les demandes et méthodes dont le temps de réponse est supérieur à 1 milliseconde sont tracées. La valeur par défaut est `0`, ce qui signifie que la trace de méthode est activée pour toutes les demandes et méthodes.
kkm_min_wallclock_to_include_stacks	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en secondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. Si vous définissez cette variable sur 0,001, par exemple, les demandes et les méthodes dont le temps de réponse est supérieur à 1 milliseconde sont tracés. La valeur par défaut est `0`, ce qui signifie que la trace de pile est activée pour toutes les demandes et méthodes.

Annulation de la configuration du collecteur de données Ruby pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller votre environnement Ruby ou si vous souhaitez mettre à niveau le collecteur de données Ruby, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Ruby.

Procédure

1. Accédez au dossier principal de l'application.
2. Supprimez les lignes suivantes de `Gemfile` dans le dossier de base de votre application Ruby :

```
gem 'logger',  '>= 1.2.8'
source 'https://maagemserver.ng.bluemix.net/' do
  gem 'ibm_resource_monitor'
  gem 'stacktracer'
end
```

3. Exécutez la commande `bundle lock`.
4. A partir du répertoire de base de l'application, exécutez la commande suivante pour renvoyer l'application par push à IBM Cloud afin que les modifications soient prises en compte.

```
cf push
```

Résultats

Vous avez correctement annulé la configuration du collecteur de données Ruby.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Configuration de la surveillance de SAP

Pour surveiller un système SAP, l'Monitoring Agent for SAP Applications doit se connecter à un serveur d'applications sur le système à surveiller afin que l'agent puisse accéder au code Advanced Business Application Programming (ABAP) fourni avec le produit.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for SAP agent
- L'agent SAP ne prend pas en charge les systèmes SAP non Unicode.

Pourquoi et quand exécuter cette tâche

L'Agent SAP est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
  - «Configuration de l'agent sur des systèmes Windows», à la page 682
  - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 683
- Pour configurer l'agent sur des systèmes d'exploitation Linux ou AIX, vous pouvez exécuter le script et répondre aux invites ou utiliser le fichier de réponses silencieux.
  - «Configuration de l'agent sur des systèmes Linux ou AIX», à la page 683
  - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 683

Une fois que vous avez installé l'agent SAP, vous pouvez importer le transport ABAP (Advanced Business Application Programming) sur le système SAP pour prendre en charge la collecte des données sur le système SAP. Pour plus d'informations, voir «Importation du transport ABAP dans le système SAP», à la page 687.

Une fois que vous avez configuré l'agent SAP, vous devez vérifier sa configuration. Pour plus d'informations, voir «Vérification de la configuration de l'agent», à la page 694.

Après avoir configuré l'agent SAP, vous pouvez ajouter le numéro de port de communication de la base de données qui est requis pour la conformité avec OSLC (Open Source Lifecycle Collaboration). Pour plus d'informations, voir «Ajout du numéro de port de communication de base de données», à la page 698.

Pour supprimer le transport ABAP du système SAP, vous devez importer le transport DELETE dans le système SAP. Pour plus d'informations, voir «Suppression du transport ABAP du système SAP», à la page 693.

La nouvelle conception CCMS est activée par défaut. Une entrée est présente dans la table de base de données /ibmmon/itm_cngf pour le paramètre isnewccmsdesign dont la valeur est définie sur yes.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent SAP sur des systèmes Windows à l'aide de la fenêtre IBM Performance Management afin que l'agent puisse collecter des données à partir du serveur d'applications SAP surveillé.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**. La fenêtre Agent de surveillance pour SAP Applications s'affiche.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système (SID) à 3 chiffres du serveur d'applications SAP géré. Par exemple, si l'identificateur système (SID) du serveur d'applications SAP géré est PS1, entrez `PS1` comme nom d'instance.
4. Configurez l'Agent SAP en mode Serveur d'applications ou Groupe de connexions.
   - Procédez comme suit pour configurer l'Agent SAP en mode Serveur d'applications :
     a. Dans la zone **Mode de connexion**, sélectionnez **Mode Serveur d'applications** et cliquez sur **Suivant**.
     b. Dans la section **Specify Application Server Information**, indiquez des valeurs pour des paramètres de configuration et cliquez sur **Suivant**.
     c. Dans la zone **Specify Logon Information to the SAP System**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 684
   - Procédez comme suit pour configurer l'Agent SAP en mode Groupe de connexions :
     a. Dans la zone **Mode de connexion**, sélectionnez **Mode Groupe de connexions** et cliquez sur **Suivant**.
     b. Dans la section **Specify Logon Group Information**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **Suivant**.
     c. Dans la zone **Specify Logon Information to the SAP System**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 684

   Important : Pour le mode Serveur d'applications, il est obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré. Pour le mode Groupe de connexions, il n'est pas obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré.
5. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

   Important : Si vous souhaitez créer une autre instance de l'Agent SAP, répétez les étapes 1 à 6. Utilisez un identificateur système unique pour chaque instance d'Agent SAP que vous souhaitez créer.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Linux ou AIX

Vous pouvez configurer l'Agent SAP sur des systèmes Linux ou AIX pour que l'agent puisse collecter des données du serveur d'applications SAP surveillé.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance : `./sap-agent.sh config nom_instance`

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système (SID) à 3 chiffres du serveur d'applications SAP géré. Par exemple, si l'identificateur système (SID) du serveur d'applications SAP géré est PS1, entrez `PS1` comme nom d'instance.
3. Lorsque la ligne de commande affiche le message suivant, entrez `1` et appuyez sur Entrée : `Edit 'Monitoring Agent for SAP Applications' setting? [1=Yes, 2=No]`
4. Configurez l'Agent SAP à l'aide du mode Serveur d'applications ou du mode Groupe de connexions.
   - Procédez comme suit pour configurer l'Agent SAP en mode Serveur d'applications :
     a. Lorsque la ligne de commande affiche le message suivant, entrez `1` et appuyez sur Entrée : `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Indiquez les valeurs des paramètres de configuration.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 684.
   - Procédez comme suit pour configurer l'Agent SAP en mode Groupe de connexions :
     a. Lorsque la ligne de commande affiche le message suivant, entrez `2` et appuyez sur Entrée : `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Indiquez les valeurs des paramètres de configuration.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 684.

   Important : Pour le mode Serveur d'applications, il est obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré. Pour le mode Groupe de connexions, il n'est pas obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré.
5. Exécutez la commande suivante pour démarrer l'Agent SAP : `./sap-agent.sh start nom_instance`

   Important : Si vous souhaitez créer une autre instance de l'Agent SAP, répétez les étapes 1 à 5. Utilisez un identificateur système unique pour chaque instance d'Agent SAP que vous créez.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Vous pouvez configurer l'Agent SAP sur des systèmes Windows, Linux ou AIX à l'aide du fichier de réponses silencieux.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `sap_silent_config.txt` disponible dans le chemin d'accès *rép_install*`\samples` et indiquez les valeurs pour tous les paramètres de configuration.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent»
2. Sur la ligne de commande, accédez au répertoire bin :

   Windows *rép_install*`\BIN`

   Linux AIX *rép_install*`\bin`
3. Exécutez la commande suivante :

   Windows `sap-agent.bat config` *nom_instance rép_install*`\samples\sap_silent_config.txt`

   Linux AIX `sap-agent.sh config` *nom_instance rép_install*`\samples\sap_silent_config.txt`

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système (SID) à 3 chiffres du serveur d'applications SAP géré. Par exemple, si l'identificateur système (SID) du serveur d'applications SAP géré est PS1, entrez `PS1` comme nom d'instance.
4. Démarrez l'agent.

   Windows Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.

   Linux AIX Exécutez la commande suivante : `./sap-agent.sh start` *nom_instance*

   Important : Si vous souhaitez créer une autre instance de l'Agent SAP, répétez les étapes 1 à 4. Utilisez un identificateur système unique pour chaque instance d'Agent SAP que vous créez.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent SAP, vous pouvez modifier la valeur par défaut des paramètres, comme le nom d'hôte SAP et le numéro de système SAP.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'Agent SAP.

Tableau 162. Noms et descriptions des paramètres de configuration de l'Agent SAP

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP Hostname (Primary)	Nom d'hôte du serveur d'applications SAP auquel cet agent se connecte. Si vos serveurs SAP dialoguent à travers un réseau local privé, les ordinateurs hébergeant les serveurs comportent au moins deux cartes de réseau. Pour le nom d'hôte, entrez un nom permettant d'atteindre le serveur d'applications à partir de systèmes externes tels que la connexion SAPGUI. N'utilisez pas le nom d'hôte du réseau LAN privé. Le nom d'hôte par défaut est celui sur lequel l'agent est installé.	Oui	`saphost.domain.com`

Tableau 162. Noms et descriptions des paramètres de configuration de l'Agent SAP (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP System Number (Primary)	Numéro de système SAP ou numéro d'instance à deux chiffres utilisé pour la connexion à un serveur hôte SAP. La valeur par défaut est 00.	Oui	
SAP Hostname (Alternate 1)	(facultatif) Deuxième choix pour le nom d'hôte si l'hôte principal est indisponible.	Non	
SAP System Number (Alternate 1)	Premier numéro de système de remplacement pour le nom d'hôte.	Non	
SAP Hostname (Alternate 2)	Troisième choix pour le nom d'hôte si le nom d'hôte SAP (Principal) et le nom d'hôte SAP de remplacement (Remplacement 1) sont indisponibles.	Non	
SAP System Number (Alternate 2)	Second numéro de système de remplacement pour le nom d'hôte.	Non	
SAP Client Number	Numéro de client SAP pour la connexion RFC à SAP. La valeur par défaut est 000. Si l'utilisateur IBMMON_AGENT généré par ABAP est utilisé, entrez le numéro de client qui a été spécifié dans l'importation de transport. Ce numéro est le même que le numéro de client nnn sous le profil.	Oui	
SAP User Id	Identificateur utilisateur SAP pour la connexion RFC à SAP. La valeur par défaut est IBMMON_AGENT, c'est-à-dire l'ID utilisateur prédéfini qui est créé lors de l'importation.	Oui	
SAP User Password	Utilisez le mot de passe par défaut ou indiquez un mot de passe différent.	Oui	
Confirm SAP User Password	Mot de passe indiqué dans la zone **SAP User Password**.	Oui	

Tableau 162. Noms et descriptions des paramètres de configuration de l'Agent SAP (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP Language Code	Code de langue qui indique la langue que l'agent utilise lors la connexion au système SAP. La langue indiquée détermine celle dans laquelle s'affichent les informations SAP, comme les messages d'alerte, les messages syslog et les messages du journal des travaux. Tous les systèmes SAP sont fournis en anglais et en allemand. Si vous avez besoin d'une langue différente, vérifiez auprès de votre administrateur SAP que cette langue est installée sur le système SAP. Si vous indiquez une langue qui n'est pas prise en charge, l'agent ne peut pas se connecter au système SAP. Les langues et codes suivants sont pris en charge : • CS - tchèque • EN - anglais • FR - français • DE - allemand • HU - hongrois • IT - italien • ES - espagnol • JA - japonais • KO - coréen • PL - polonais • PT - portugais • RU - russe • ZH - chinois • ZF - chinois traditionnel	Oui	
RFC Trace	Paramètre de trace RFC (Remote Function Call) pour la variable *SAPTRACE*. Lorsque vous cochez cette case, vous activez la fonction de trace RFC et la valeur par défaut est aucun traçage RFC. Pour la ligne de commande, 2 = pas de trace et 1 = trace. Dans la mesure où la fonction de trace RFC génère des informations de diagnostics étendues, utilisez-la soigneusement. Pour plus d'informations sur la fonction de trace RFC, contactez le support IBM.	Non	
SAP Logon Group	Nom du groupe relatif aux connexions de serveur SAP.	Oui	
SAP Message Server Name	Nom d'hôte du serveur de messages SAP.	Oui	

Tableau 162. Noms et descriptions des paramètres de configuration de l'Agent SAP (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP Message Service	Nom du service où se trouve le serveur de messages SAP. Vous devez inclure les noms de service dans les fichiers de services du système d'exploitation suivants : • `/etc/services` • `\windows\system32\drivers\etc\services`	Oui	Vous pouvez utiliser le nom de service de messages sapmsTV1, ou le numéro de port du service de messages complet 3601.
SAP Route String	Si vous devez accéder au serveur SAP qui utilise un routeur SAP, vous devez indiquer la chaîne du routeur SAP.	Non	La chaîne de routeur `/H/host/H/` doit être au format suivant : `/H/beagle/H/ brittany/H/` ou `/H/amsaix11.tivlab. raleigh.ibm.com/W/ tivoli/H/amsaix25`
SNC	Indiquez si vous souhaitez activer ou désactiver SNC (Secure Network Communications). La valeur par défaut est Disabled (désactivé).	Oui	**`sap_conn.sap_snc_mode`** `=true` ou `false`
SNC Security Level	Niveau de sécurité de SNC.	Oui	**`sap_snc_mode1.sap_snc _qop`**=*valeur_QOP*. La valeur par défaut est 8.
Client or Agent SNC Name	Nom SNC du client ou de l'agent.	Oui	**`sap_snc_mode1.sap_snc _client`**= *nom_SNC_client*
Partner or SAP Server SNC Name	Nom SNC du partenaire ou du serveur SAP.	Oui	**`sap_snc_mode1.sap_snc _server`**= *nom_SNC_serveur*
SAP Cryptolibrary Path	Chemin de la bibliothèque cryptographique SAP.	Oui	**`sap_snc_mode1.sap_snc _library`**= *Chemin_bibliothèque_cryptographique*

Importation du transport ABAP dans le système SAP

Vous pouvez installer un agent Agent SAP pour chaque système SAP sur lequel vous importez la demande de transport ABAP (Advanced Business Application Programming) pour prendre en charge la collecte des données sur le système SAP.

Avant de commencer

Avant d'importer le transport ABAP sur le système SAP, assurez-vous que les prérequis suivants sont respectés :

- Pour importer la demande de transport de produit, R3trans Version 01.07.04 ou ultérieure est requis car les tables Dynpro et Exportation et Importation sont incompatibles. Le fonctionnement de base de l'agent n'est pas affecté par les problèmes d'incompatibilité Dynpro ou Exportation et Importation ; seules les fenêtres de configuration SAP sont affectées.
- Pour surveiller le système Solution Manager, veillez à bien importer le transport Agent SAP version 7.1.1 sur le client où la configuration MAI est disponible. Pour afficher les fonctions du système PI, importez le transport Agent SAP version 7.1.1 sur le système PI sur un client où la configuration PI est disponible.

- Pour afficher les données dans les widgets de groupe qui se trouvent sous le sous-noeud SLM, vous devez effectuer les configurations MAI de PI et Solution Manager. Vous devez également configurer la surveillance des processus métier afin de pouvoir afficher les données dans le widget de groupe Alertes BPM. Pour afficher les données du widget de groupe Dernières alertes critiques et de priorité élevée, procédez aux configurations suivantes :
  - Dans Solution Manager 7.1, exécutez la transaction SOLMAN_SETUP et sélectionnez **System Monitoring**, activez le composant tiers et ajoutez **Implementation: BADI Definition for Alert Reactions** et le connecteur tiers.
  - Définissez le filtre de portée à la valeur **All Alerts and Metrics**.
  - Vérifiez que l'état d'implémentation est **Actif**.

  Pour plus d'informations, reportez-vous aux notes d'OSS (Online Service System) suivantes, qui incluent une liste des niveaux de Service Pack SAP requis :
  - OSS Note 454321
  - OSS Note 330267
  - OSS Note 743155
- Pour surveiller les systèmes SAP, l'Agent SAP a besoin des données statistiques SAP. Sur les systèmes SAP 7.0, vous devez définir le fuseau horaire du système SAP afin qu'il corresponde au fuseau horaire du système d'exploitation, afin que les statistiques SAP soient collectées avec les horodatages adéquats. De même, mettez à jour le fuseau horaire du système SAP pour l'Agent SAP de sorte que ce dernier puisse collecter les données. Pour plus d'informations concernant ce sujet, consultez la note SAP 926290.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur l'importation du transport SAP, voir «Importation du transport SAP», à la page 689.

Prérequis relatifs aux alertes MAI pour l'importation du transport ABAP

Vous devez vérifier les prérequis relatifs aux alertes MAI avant d'importer le transport ABAP.

Paramètres de configuration dans le fichier `transport.prop`

Lorsque vous utilisez le nouveau mécanisme d'extraction des alertes MAI qui permet d'extraire les alertes MAI sans avoir à configurer les paramètres de notification par e-mail et sans implémentation BAdi, vous devez modifier le paramètre de configuration suivant dans le fichier `transport.prop`.

Ajoutez la ligne SPLEVEL=X, où X correspond au niveau de module de support (SP) du système Solution Manager.

Par exemple, si l'ID système est S10 et que le niveau de module de support est 13, ajoutez SPLEVEL=13.

Important : Pour un système SAP avec un niveau SP 10 ou ultérieur, la valeur de l'attribut Technical Name (MEA) n'est pas renseignée dans le widget de groupe Latest MAI Alerts with Rating 'Red' du tableau de bord SAP Solution Manager lorsque les alertes MAI sont extraites sans configurer les notifications par e-mail dans SAP Solution Manager et sans implémentation BAdi. La valeur de l'attribut Technical Name (MEA) est renseignée dans le widget de groupe Latest MAI Alerts with Rating 'Red' du tableau de bord SAP Solution Manager lorsque les alertes MAI sont extraites en configurant les notifications par e-mail dans SAP Solution Manager et l'implémentation BAdi.

Détermination des anciens et des nouveaux mécanismes d'extraction des alertes MAI en fonction du niveau de module de support (SP) Solution Manager

Ancien mécanisme d'extraction des alertes MAI
Ce mécanisme se base sur la configuration des paramètres de notification par e-mail et sur l'implémentation BAdi /IBMMON/ITM_IMPL_ALRTINBX avec l'interface IF_ALERT_DYN_COFIGURATION pour collecter les alertes MAI et les envoyer à l'Agent SAP.

Nouveau mécanisme d'extraction des alertes MAI
Ce mécanisme se base sur l'extraction des alertes MAI sans avoir à configurer les paramètres de notification par e-mail et sans implémentation BAdi /IBMMON/ITM_IMPL_ALRTINBX avec l'interface IF_ALERT_DYN_COFIGURATION.

Vous pouvez utiliser le tableau ci-dessous pour comprendre l'utilisation du fichier `transport.prop` et sa dépendance à la configuration des paramètres de notification par e-mail.

Tableau 163. Utilisation du fichier transport.prop et ses dépendances

Niveau SP du système SAP	Paramètres transport.prop		Configuration des paramètres de notification par e-mail	Mécanisme d'extraction des alertes MAI à utiliser
	MAI_ CONFIGURED	Niveau SP de Solution Manager		
Tous	No ou file does not exist	Non applicable	Configurés ou non	Le sous-noeud SOL apparaît à la place du sous-noeud SLM.
SP 6 à 9	Yes	Mentionné	Configurés	Ancien mécanisme
SP 6 à 9	Yes	Non mentionné	Configurés	Ancien mécanisme
SP 6 à 9	Yes	Non mentionné	Non configurés	L'ancien mécanisme ne fonctionne pas car la configuration des paramètres de notification par e-mail est obligatoire.
SP 6 à 9	Yes	Mentionné	Non configurés	L'ancien mécanisme ne fonctionne pas car la configuration des paramètres de notification par e-mail est obligatoire.
SP 10 ou ultérieur	Yes	Mentionné	Configurés	Nouveau mécanisme
SP 10 ou ultérieur	Yes	Mentionné	Non configurés	Nouveau mécanisme
SP 10 ou ultérieur	Yes	Non mentionné	Configurés	Ancien mécanisme
SP 10 ou ultérieur	Yes	Non mentionné	Non configurés	L'ancien mécanisme ne fonctionne pas car la configuration des paramètres de notification par e-mail est obligatoire.

Importation du transport SAP

L'Agent SAP fournit un ensemble de routines ABAP (Advanced Business Application Programming) pour prendre en charge la collecte des données dans le système SAP. Ce code ABAP est distribué comme transport SAP qui doit être installé sur chaque système SAP à surveiller. Votre administrateur SAP installe le transport.

Pourquoi et quand exécuter cette tâche

Le profil d'autorisation **ZITM_610AUTH** et le rôle d'autorisation **ZITM_610AUT** ne sont valides que jusqu'à la version 6.1. A partir de la version 6.2 ou d'une version ultérieure, le profil d'autorisation **/IBMMON/AUTH** est utilisé. Pour se protéger contre une utilisation par une personne non autorisée, le code ABAP qui est installé sur le système SAP n'est pas visible de l'intérieur du système SAP. En outre, ce code ne peut être ni modifié, ni généré. Vous devez obtenir le support de ce code à partir du site Web de support des logiciels IBM.

En plus d'installer le code ABAP, le transport installe également les éléments de texte traduits dans le cadre de la prise en charge multiculturelle des éléments de texte du transport SAP.

Important : Avant d'importer le transport dans le système SAP, vous ne devez pas démarrer l'instance Agent SAP configurée pour surveiller le système SAP.

Lorsque vous importez le transport SAP, les utilisateurs sont définis de manière implicite dans le système SAP.

Procédez comme suit pour importer le transport SAP dans le système SAP.

Procédure

1. Copiez le fichier de transport IBM Tivoli Monitoring à partir des chemins ci-après, sur l'ordinateur où l'agent est installé.
   - Pour les systèmes d'exploitation Windows : *rép_install*\TMAITM6_x64\ABAP
   - Pour les systèmes d'exploitation non Windows : *rép_install*/*intrp*/sa/ABAP, où *intrp* doit être **lx8266** ou **aix526**.
2. Copiez les fichiers de transport suivants des chemins mentionnés à l'étape 1 dans l'environnement SAP :
   - K711_00xxxU.ITM et R711_00xxxU.ITM

     Ces fichiers sont des versions Unicode du transfert. Ils contiennent le code ABAP de l'Agent SAP, ainsi que la prise en charge Unicode des chaînes de texte pour les pages de codes latins et les pages de codes sur deux octets.
   - K711_00xxx_DELETE.ITM et R711_00xxx_DELETE.ITM

     Ces fichiers suppriment le code ABAP. Il n'est pas nécessaire d'importer le transport DELETE, à moins que vous n'arrêtiez d'utiliser intégralement le produit et que vous souhaitiez supprimer les transports des systèmes SAP. Voir «Suppression du transport ABAP du système SAP», à la page 693
3. Copiez vos fichiers de transport dans le répertoire de données du système de transport SAP comme indiqué ci-dessous, sans modifier le nom du fichier de transport :

   Transport Unicode
   a. Copiez le fichier K711_00xxxU.ITM dans le répertoire cofiles.
   b. Copiez le fichier R711_00xxxU.ITM dans le répertoire data.
4. Pour installer l'unique fichier de transport IBM Tivoli Monitoring sur le système SAP, sélectionnez l'une des options d'importation de fichier suivantes :
   - Pour le système SAP qui correspond à un niveau Solution Manager 7.1 Service Pack 6 ou ultérieur et pour lequel MAI est configuré, vous devez créer le fichier transport.prop dans le répertoire de travail usr/sap/SID/DVEBMGS*numéro_instance*/work du système SAP. Si le système SAP est un système réparti avec ASCS (ABAP SAP Central Services), créez le fichier transport.prop dans le répertoire usr/sap/SID de l'instance centrale. Ajoutez ensuite l'entrée MAI_CONFIGURED = YES dans ce fichier. Cette entrée crée une entrée MAI_CONFIGURED = YES dans la table /IBMMON/ITM_CNFG. Vous pouvez maintenant importer l'unique fichier de transport IBM Tivoli Monitoring sur le système SAP.

Remarque : Avant d'importer ce fichier de transport IBM Tivoli Monitoring, vous devez créer le fichier `transport.prop` dans le répertoire de travail `usr/sap/SID/DVEBMGS`*`numéro_instance`*`/work` du système SAP et ajouter l'entrée `MAI_CONFIGURED = YES` dans ce fichier. Vous ne devez pas éditer l'entrée dans la table `/IBMMON/ITM_CNFG`.

- Pour tous les autres systèmes SAP dont la version de base correspond à la version 7.0 ou une version ultérieure et qui disposent de Solution Manager version 7.1 sans configuration MAI, vous devez importer directement l'unique fichier de transport IBM Tivoli Monitoring.

5. Exécutez la commande suivante pour importer le transport SAP :

```
tp addtobuffer ITMK711_00xxxU SID
pf=\usr\sap\trans\bin\NOM_PROFIL
```

où :

SID Correspond à l'ID du système SAP cible.

NOM_PROFIL
Correspond au nom du fichier de profil tp. Vérifiez que le fichier de paramètres tp actuel est spécifié lorsque vous importez les fichiers de transport d'agent à partir de la ligne de commande. Le fichier de paramètres tp est généralement nommé `TP_DOMAIN_`*`SID`*`.PFL`. Ce nom de fichier est sensible à la casse sous UNIX.

nnn Numéro du client cible sur lequel l'agent est exécuté et pour lequel l'ID utilisateur, IBMMON_AGENT, le profil d'autorisation et `/IBMMON/AUTH` sont définis.

Vous pouvez également utiliser la transaction STMS de SAP pour importer les demandes de transport ITMK711_00xxxU.ITM. Vérifiez que les options ci-après sont sélectionnées dans l'onglet **Import Options** de la fenêtre Import Transport Request.

- **Leave Transport Request in Queue for Later Import**
- **Import Transport Request Again**
- **Overwrite Originals**
- **Overwrite Objects in Unconfirmed Repairs**

Pour la version de base de SAP, si l'option **Ignore Invalid Component Version** est activée, vérifiez qu'elle est sélectionnée.

Résultats

En fonction du niveau de votre version SAP, lorsque vous exécutez la commande **`tp import`**, vous risquez de recevoir le code retour 4, qui n'indique pas de problème. L'affichage du code retour 4 est le résultat attendu après l'exécution de la commande **`import`**.

Utilisateurs et autorisations nécessaires pour l'Agent SAP

Si vous souhaitez vous protéger contre l'accès non autorisé au système SAP, vous pouvez affecter des autorisations à l'utilisateur qui se connecte à celui-ci. Ces autorisations définissent les niveaux d'accès de l'utilisateur dans le système SAP.

Après l'importation du transport ABAP, l'agent SAP crée l'ID utilisateur par défaut IBMMON_AGENT dans le système SAP ainsi que le mot de passe par défaut ITMMYSAP. Cet utilisateur est un utilisateur système auquel est associé le profil d'autorisation /IBMMON/AUTH. Le profil /IBMMON/AUTH et l'utilisateur IBMMON_AGENT sont créés à l'issue de l'importation du transport ABAP. Avec le profil /IBMMON/AUTH, l'utilisateur IBMMON_AGENT peut accéder aux transactions qui sont nécessaires pour lire les données de performances depuis le système SAP. Voici ci-dessous quelques exemples des transactions utilisées :

- Alertes et administration CDSM
- Autorisation de surveillance des messages PI/XI
- Autorisations Solution Manager

Vous pouvez créer un autre utilisateur de type système pour l'agent. L'utilisateur doit être associé au profil /IBMMON/AUTH.

Pour visualiser les données des composants SAP et y accéder, assurez-vous que l'utilisateur créé pour l'agent dispose de toutes les autorisations mentionnées dans le tableau suivant :

Tableau 164. Liste des autorisations

Composants	Objets d'autorisation	Description de l'autorisation
Autorisations système générales comprenant les composants suivants : • Instance SAP • Système SAP	S_ADMI_FCD	Permet d'accéder au système SAP
	S_BDS_DS -BC-SRV-KPR-BDS	Permet d'accéder à l'ensemble de documents
	S_BTCH_JOB	Permet d'exécuter des opérations sur des travaux en arrière-plan
	S_CCM_RECV	Permet de transférer les données de référentiel du système central
	S_C_FUNCT	Permet d'effectuer des appels aux fonctions de noyau C dans les programmes ABAP
	S_DATASET	Permet d'accéder aux fichiers
	S_RFC	Permet de vérifier l'accès RFC. L'objet d'autorisation S_RFC contient les deux sous-autorisations suivantes : • RFC1 : pour fournir les autorisations pour le groupe de fonctions RFC1. • SDIFRUNTIME : pour fournir les autorisations pour le groupe de fonctions SDIFRUNTIME.
	S_RFCACL	Permet de vérifier l'autorisation des utilisateurs de RFC
	S_RZL_ADM	Permet d'accéder au système CCMS (Computing Center Management System) pour l'administration de R/3 System
	S_TCODE	Permet de vérifier les autorisations de démarrage des transactions qui sont définies pour une application
	S_TOOLS_EX	Permet d'afficher les enregistrements de statistiques externes dans des outils de surveillance
Autorisations pour PI comprenant l'intégration des processus SAP	S_XMB_MONI	Permet d'accéder à la surveillance des messages XI

Tableau 164. Liste des autorisations (suite)

Composants	Objets d'autorisation	Description de l'autorisation
Autorisations pour MAI comprenant SAP Solution Manager	AI_DIAGE2E	Permet de restreindre les fonctions de diagnostics d'E2E
	AI_LMDB_OB	Permet d'accéder aux objets LMDB (Landscape Management Database)
	SM_MOAL_TC	Permet de contrôler l'accès aux fonctionnalités d'alerte et de surveillance de SAP Solution Manager
	SM_WC_VIEW	Permet de restreindre l'accès aux éléments d'interface utilisateur spécifiques dans les centres de charge de Solution Manager
	S_RFC_ADM	Permet de contrôler les droits d'administration des destinations RFC
	S_RS_AUTH	Permet de spécifier les autorisations d'analyse au sein d'un rôle
	SM_APPTYPE	Permet d'accéder au type d'application Solution Manager
	SM_APP_ID	Permet d'accéder aux applications fournies dans les centres de charge

Suppression du transport ABAP du système SAP

Si vous choisissez de supprimer l'Agent SAP de votre système, vous devez importer le transport DELETE sur le système SAP. Ce transport supprime les objets dictionnaire et modules de fonction de l'Agent SAP.

Avant de commencer

Avant de supprimer le transport du système SAP, vous devez arrêter l'instance Agent SAP configurée pour surveiller le système SAP.

Si le système SAP est de version 7.20 ou ultérieure, avant d'importer le transport DELETE, vous devez ajouter le paramètre de profil de transport **tadirdeletions=true** dans votre profil de transport. Ce paramètre est disponible sur tp version 375.57.68 et également dans R3trans version 6.14 édition 700 ou suivante. Pour plus d'informations sur la suppression de demandes de transport du système SAP, voir Suppression de demandes de transport.

Procédure

1. Accédez au chemin suivant :
   - Pour les systèmes d'exploitation Windows : *rép_install*\TMAITM6_x64\ABAP
   - Pour les systèmes d'exploitation non Windows : *rép_install*/*intrp*/sa/ABAP, où *intrp* doit être **lx8266** ou **aix526**.
2. Copiez les fichiers de transfert dans l'environnement SAP.
3. Copiez les fichiers K711_00xxx_DELETE et R711_00xxx_DELETE dans le répertoire de données du système de transfert SAP, comme suit :
   a. Copiez le fichier K711_00xxx_DELETE dans le répertoire cofiles.
   b. Copiez le fichier R711_00xxx_DELETE dans le répertoire data.
4. Exécutez les commandes suivantes pour importer le transport DELETE :

a. **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin***NOM_PROFIL*

b. **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *NOM_PROFIL*, où :

SID Correspond à l'ID du système SAP cible.

NOM_PROFIL
Correspond au nom du fichier de profil tp.

nnn Correspond au numéro du client cible où l'agent doit être exécuté.

Vérification de la configuration de l'agent

Une fois que vous avez installé l'Agent SAP, vous devez vérifier sa configuration en téléchargeant, en copiant et en vérifiant la bibliothèque NetWeaver RFC SDK V7.20. Vous devez également vérifier la configuration de Solution Manager version 7.1 avec la surveillance MAI, les alertes MAI et le paramètre de configuration spécifique au composant tiers.

Vérifiez la configuration de l'agent à l'aide des procédures suivantes :

- «Téléchargement de la bibliothèque NetWeaver RFC SDK V7.20»
- «Copie de la bibliothèque NetWeaver RFC SDK V7.20 dans la configuration de l'agent SAP», à la page 695
- «Vérification de la bibliothèque NetWeaver RFC SDK V7.20», à la page 695
- «Vérification de la configuration de Solution Manager version 7.1 avec la surveillance MAI», à la page 696
- «Vérification des alertes MAI», à la page 697
- «Vérification des paramètres de configuration spécifiques au composant tiers», à la page 697

Téléchargement de la bibliothèque NetWeaver RFC SDK V7.20

Téléchargez la bibliothèque NetWeaver RFC SDK V7.20 une fois l'installation de l'agent SAP terminée. Tous les fichiers liés à la bibliothèque NetWeaver RFC SDK V7.20 peuvent être téléchargés à partir du site Web de SAP.

Procédure

1. Connectez-vous à SAP Marketplace avec l'adresse URL suivante : http://service.sap.com
2. Cliquez sur **SAP Support Portal**.
3. Entrez votre nom d'utilisateur et votre mot de passe Service Marketplace.
4. Cliquez sur **Software Downloads** et développez le lien **Support Packages and Patches**.
5. Cliquez sur **Browse our Download Catalog**, puis cliquez sur **Additional Components**.
6. Cliquez sur **SAP NetWeaver RFC SDK**, puis cliquez sur **SAP NetWeaver RFC SDK 7.20**.
7. Sélectionnez le système d'exploitation sur lequel se trouve l'agent SAP.
8. Téléchargez le fichier `*.SAR` sur votre ordinateur.
9. Pour extraire le fichier `SAP Netweaver RFC SDK *.SAR` avec l'utilitaire SAPCAR mis à disposition par SAP, exécutez la commande suivante :
   `sapcar -xvf` *`nom du fichier SAP NetWeaver RFC SDK`*`.SAR`

   Remarque : Vous pouvez télécharger l'utilitaire SAPCAR depuis le site Web SAP.
10. Accédez au dossier `lib` dans le dossier extrait.

Que faire ensuite

Copiez la bibliothèque NetWeaver RFC SDK V7.20 dans la configuration de l'agent SAP.

Copie de la bibliothèque NetWeaver RFC SDK V7.20 dans la configuration de l'agent SAP

La bibliothèque NetWeaver RFC SDK V7.20 contient des fichiers que vous devez copier manuellement à l'emplacement de la configuration de l'agent SAP.

Procédure

1. Accédez au répertoire dans lequel vous avez téléchargé la bibliothèque NetWeaver RFC SDK V7.20.
2. Copiez les fichiers à l'emplacement de la configuration de l'agent SAP.
   - Pour les systèmes d'exploitation Windows 64 bits, vous devez copier les fichiers suivants :
     - `icuin34.dll`
     - `libicudecnumber.dll`
     - `libsapucum.dll`
     - `icudt34.dll`
     - `icuuc34.dll`
     - `sapnwrfc.dll`

     Vous devez copier les fichiers à l'emplacement `rép_install\TMAITM6_x64`.
   - Pour les systèmes d'exploitation autres que Windows, vous devez copier les fichiers dans `rép_install/`*`intrp`*`/sa/lib`, où *intrp* est le code du système d'exploitation (aix526, li6263, sol606). Vous devez copier les fichiers suivants :
     - `libsapnwrfc.so`
     - `ibicudecnumber.so`
     - `ibicuuc34.a`
     - `libicui18n34.a`
     - `libicudata34.a`
     - `libsapucum.so`

Que faire ensuite

Vérifiez la version de la bibliothèque NetWeaver RFC SDK V7.20 téléchargée.

Vérification de la bibliothèque NetWeaver RFC SDK V7.20

Vous devez vérifier la version du fichier après avoir copié le fichier extrait.

Procédure

- Windows Pour vérifier la version du fichier, procédez comme suit :
  1. Cliquez avec le bouton droit de la souris sur `sapnwrfc.dll`, puis cliquez sur **Propriétés**.
  2. Cliquez sur l'onglet **Version**.
  3. Dans la section **Version du produit**, vérifiez que la version est la suivante : 720, patch 514, changelist 1448293 (ou qu'il s'agit d'une version ultérieure).
- Linux AIX Pour vérifier la version du fichier, procédez comme suit :
  1. Accédez au dossier `lib` dans le fichier `*.SAR` extrait.
  2. Exécutez la commande suivante : **`strings libsapnwrfc.so | grep SAPFileVersion`**
  3. Le message suivant doit s'afficher : `[root@IBMSAP2V6 lib]# strings libsapnwrfc.so | grep SAPFileVersion GetSAPFileVersion #[%]SAPFileVersion: 7200, 514, 22, 6206 .GetSAPFileVersion`

  Remarque : Le message indique que la version de cette bibliothèque est la version 720 correctif 514 (ou une version ultérieure).

Vérification de la configuration de Solution Manager version 7.1 avec la surveillance MAI

Afin de recevoir des données pour les alertes MAI, vous devez vérifier que Solution Manager version 7.1 est configuré correctement.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser Solution Manager version 7.1 avec MAI (Monitoring and Alerting Infrastructure) pour surveiller les systèmes gérés. Solution Manager version 7.1 se surveille lui-même ainsi que les systèmes satellites. Chaque système satellite possède un plug-in et des agents de diagnostic. Les agents de diagnostic extraient les données de niveau hôte ou système d'exploitation. Chaque hôte peut posséder plusieurs agents de diagnostic pour différentes instances de Solution Manager surveillant l'hôte. Vous trouverez ci-après les mots clés qui sont utilisés dans la surveillance MAI de Solution Manager :

- Mesures : données provenant des systèmes satellites.
- Alertes : notifications reposant sur des dépassements de valeurs de seuil pouvant être configurées.
- Incident : alertes converties en tickets et affectées à un utilisateur.

Pour vérifier la configuration de Solution Manager version 7.1 avec la surveillance MAI, vous devez vérifier les paramètres de base, les paramètres de niveau global et les paramètres au niveau du modèle.

Procédure

1. Pour vérifier les paramètres de base, entrez le code de transaction `SOLMAN_SETUP` et appuyez sur **Entrée**. Vérifiez que tous les voyants sont verts dans les onglets suivants :
   - Overview
   - Basic Configuration
   - Managed System Configuration

   Remarque : Il existe différentes catégories de systèmes gérés : systèmes techniques, scénarios techniques, hôte, base de données, instance, domaine PI, composant technique et connexion. Vous devez configurer ces systèmes gérés en fonction des besoins métier. Les alertes MAI reposent sur les systèmes gérés que vous avez configurés.
2. Entrez le code de transaction `SE38` et appuyez sur **Entrée**.
3. Indiquez le nom de programme `RTCCTOOL` et exécutez le rapport. Vérifiez que tous les voyants sont verts dans la sortie.
4. Pour vérifier les paramètres globaux, entrez le code de transaction : `SOLMAN_WORKCENTER` et cliquez sur **Entrée**. Vérifiez que tous les voyants sont verts dans les onglets suivants :
   - Overview
   - Configure Infrastructure
   - Pre-requisites
   - Configurer
5. Vérifiez si **Global Settings** pour le statut **Notification** est **Active**.
6. Pour vérifier les paramètres au niveau du modèle, entrez le code de transaction `SOLMAN_SETUP` et cliquez sur **Entrée**. Dans **Technical Settings**, dans la liste **Auto-Notifications**, vérifiez que **Active** est sélectionné.

   Remarque : Pour un traitement initial des incidents, vérifiez que les notifications par courrier électronique sont actives.
7. Pour la surveillance de système MAI, vérifiez la configuration d'End-User Experience Monitoring (EEM) en procédant comme suit :
   a. Entrez le code de transaction `SE37` et appuyez sur **Entrée**.

b. Entrez **AI_EEM_LIST_ALL_SCENARIOS** dans la zone **Function Module name** et appuyez sur F8. Une entrée pour End-User Experience Monitoring (EEM) doit exister.

Vérification des alertes MAI

Pour vous assurer que l'infrastructure MAI de Solution Manager est configurée correctement pour la surveillance de la boîte de réception des alertes MAI dans Technical Monitoring, vous devez vérifier que vous recevez les alertes MAI dans la sortie.

Procédure

1. Entrez le code de transaction SOLMAN_WORKCENTER et appuyez sur **Entrée**. Vérifiez si vous pouvez afficher les alertes MAI dans la boîte de réception des alertes MAI de Solution Manager, sous Technical Monitoring.
2. Recherchez l'implémentation BADI en procédant comme suit :
   a. Entrez le code de transaction SE19 et appuyez sur **Entrée**.
   b. Entrez /IBMMON/ITM_IMPL_ALRTINBX dans la zone **Enhancement Implementation**.
   c. Cliquez sur **Display** et vérifiez si l'implémentation BADI est active dans la section **Runtime Behavior**.
3. Vérifiez si la base de données /IBMMON/ITM_ALIX contient des alertes MAI, à l'aide des étapes suivantes :
   a. Entrez le code de transaction SE16 et appuyez sur **Entrée**.
   b. Dans la zone **Table Name**, entrez /IBMMON/ITM_ALIX et exécutez cette commande. Vérifiez que vous recevez les alertes MAI dans la table.
4. Entrez le code de transaction SE37 et appuyez sur **Entrée**.
5. Dans la zone **Function Module Name**, entrez /IBMMON/ITM_MAIALRT_INX et appuyez sur F8. Vous devez voir les alertes MAI dans la sortie.

Que faire ensuite

Si vous ne parvenez pas à voir les alertes MAI dans la base de données /IBMMON/ITM_ALIX, vous devez vérifier les paramètres dans le composant tiers.

Vérification des paramètres de configuration spécifiques au composant tiers

Si vous ne parvenez pas à voir les alertes MAI, vous devez vérifier les paramètres dans le composant tiers.

Procédure

1. Vérifiez que le composant tiers est actif.
2. Vérifiez que **Alert Reaction** est disponible dans OS Adapter, sous **BAdi Implementation**. Si tel n'est pas le cas, supprimez les paramètres par défaut et sélectionnez **BAdi implementation - Alert Reaction**.
3. Vérifiez les paramètres du modèle en procédant comme suit :
   a. Vérifiez les paramètres utilisés pour transférer des alertes spécifiques sur le système tiers, tel que SAP ABAP 7.0.0.
   b. Sélectionnez **Expert Mode**, sélectionnez **Alerts**, puis cliquez sur **Third Party Component**. Vérifiez que le nom Alert Reaction BAdi s'affiche.

      Remarque : Vérifiez que les notes SAP les plus récentes sont implémentées. Pour Solution Manager version 7.1 Service Pack 8, vérifiez que les notes suivantes sont implémentées :
      - https://service.sap.com/sap/support/notes/1959978
      - https://service.sap.com/sap/support/notes/1820727
4. Si vous ne parvenez pas à voir les alertes MAI dans la base de données /IBMMON/ITM_MAIALRT_INX, vous devez exécuter les étapes de configuration de Solution Manager MAI pour le composant tiers.

a. Entrez le code de transaction SOLMAN_SETUP et appuyez sur **Entrée**.
b. Dans Technical Monitoring, sélectionnez **System Monitoring**.
c. Cliquez sur l'onglet **Configure Infrastructure**, puis sur l'onglet **Default Settings**.
d. Cliquez sur l'onglet **Third Party Components**, puis cliquez sur **Edit**.
e. Sélectionnez **Active** dans la liste.
f. Vérifiez que le filtre de portée a pour valeur **All alerts, Events and Metrics (with Internal Events)** pour le connecteur sélectionné.

   Remarque : L'adaptateur de commande de système d'exploitation est également l'une des méthodes permettant d'envoyer des données au connecteur tiers. Pour le configurer, reportez-vous aux paramètres détaillés de la configuration dans le guide d'utilisation de l'adaptateur de commande de système d'exploitation.

Ajout du numéro de port de communication de base de données

Un numéro de port de communication de base de données est essentiel pour identifier de manière unique l'entité de base de données dans les scénarios intégrés. Pour assurer la collaboration inter-composant, les composants de SCM AI comprennent OSLC (Open Source Lifecycle Collaboration). Pour la conformité OSLC, il est essentiel d'identifier les composants de collaboration de manière unique. C'est la raison pour laquelle le numéro de port de communication de base de données est important.

Pourquoi et quand exécuter cette tâche

Lorsque vous importez le transport IBM Tivoli Monitoring approprié dans le système SAP, la table de base de données /IBMMON/ITM_PORT est créée automatiquement. Cette dernière contient les zones de base de données suivantes :

- ID système
- Nom d'hôte du système
- Numéro de port de communication de base de données

Procédure

Pour ajouter le numéro de port de communication de base de données pour l'Agent SAP qui est requis pour la conformité OSLC, procédez comme suit :

1. Accédez au code de transaction SE16 et appuyez sur la touche Entrée.
2. Dans la zone **Nom de table de base de données**, entrez /IBMMON/ITM_PORT et appuyez sur la touche F7.
3. Lorsque l'écran de sélection de la table de base de données **/IBMMON/ITM_PORT** apparaît, appuyez sur la touche F8. La table de base de données **/IBMMON/ITM_PORT** contient les trois zones de base de données suivantes :
   - ID système
   - Nom d'hôte du système
   - Numéro de port de communication de base de données

   Remarque : Les systèmes SAP qui apparaissent dans la table de base de données /IBMMON/ITM_PORT sont destinés à la fois aux architectures Java et ABAP.
4. Dans la zone **Numéro de port de communication de base de données**, entrez le numéro de port de communication de base de données SAP approprié pour l'ID système SAP et le nom d'hôte système SAP respectif et sauvegardez les modifications.

   Remarque : Si vous n'entrez pas de valeur dans la zone **Numéro de port de communication de base de données** dans la table de base de données /IBMMON/ITM_PORT, celui-ci a la valeur par défaut 0.

Configuration de la surveillance de SAP HANA Database

Vous devez configurer l'Agent SAP HANA Database pour qu'il puisse collecter les données du serveur de base de données SAP HANA surveillé.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for SAP HANA Database agent

Avant de configurer Agent SAP HANA Database, assurez-vous que les utilisateurs sont crées pour toutes les bases de données (système et titulaire) du système SAP HANA avec les privilèges suivants :

- Rôle : Surveillance
- Privilèges système : Surveillez l'administrateur

  Le nom d'utilisateur et le mot de passe pour les bases de données système et titulaire doivent être identiques.

Pourquoi et quand exécuter cette tâche

L'Agent SAP HANA Database est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Procédure

- Windows Pour configurer l'agent sur des systèmes Windows, procédez comme suit :
  1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
  2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**. La fenêtre Agent de surveillance pour SAP HANA Database s'ouvre.
  3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

     Important : Le nom d'instance de l'agent doit correspondre à l'identificateur à 3 chiffres du système de base de données HANA (SID). Par exemple, si l'ID source de la base de données gérée SAP HANA est H01, entrez `H01` comme nom d'instance.
  4. Dans la fenêtre Agent de surveillance pour SAP HANA Database, spécifiez des valeurs pour les zones suivantes :

     Nom d'instance
     La valeur par défaut de cette zone est identique à celle que vous avez indiquée dans la zone **Enter a unique instance name**.

     Nom du serveur
     Le nom de système hôte qualifié complet ou l'adresse IP du serveur SAP HANA où la base de données du système est installée.

     Nom de la base de données
     Le nom de la base de données SAP HANA.

     Numéro de port
     Numéro de port SQL du service de serveur d'index sur la base de données du système du serveur de base de données SAP HANA.

     Administrateur de la base de données HANA
     Le nom d'utilisateur pour accéder au serveur de la base de données SAP HANA.

     HANA DB Administrator Password
     Le mot de passe pour accéder au serveur de la base de données SAP HANA.

Confirm HANA DB Administrator Password
Le mot de passe indiqué dans la zone **HANA DB Administrator Password**.

5. Cliquez sur **OK**.
6. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

- Linux AIX Pour configurer l'agent sur des systèmes Linux ou AIX, procédez comme suit :
  1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
  2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance : `./sap_hana_database-agent.sh config nom_instance`

     Important : Le nom d'instance doit correspondre à l'identificateur à 3 chiffres du système de base de données HANA (SID). Si l'ID source de la base de données gérée SAP HANA est H01, entrez `H01` comme nom d'instance.
  3. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez sur Entrée : `Edit 'Monitoring Agent for SAP HANA Database' setting? [1=Yes, 2=No]`
  4. Indiquez les valeurs pour les paramètres d'agent suivants :

     Nom du serveur
     Le nom de système hôte qualifié complet ou l'adresse IP du serveur SAP HANA où la base de données du système est installée.

     Nom de la base de données
     Le nom de la base de données SAP HANA.

     Numéro de port
     Numéro de port SQL du service de serveur d'index sur la base de données du système du serveur de base de données SAP HANA.

     Administrateur de la base de données HANA
     Le nom d'utilisateur pour accéder au serveur de la base de données SAP HANA.

     HANA DB Administrator Password
     Le mot de passe pour accéder au serveur de la base de données SAP HANA.

     Confirm HANA DB Administrator Password
     Le mot de passe indiqué dans la zone **HANA DB Administrator Password** .
  5. Exécutez la commande suivante pour démarrer l'Agent SAP HANA Database : `./sap_hana_database-agent.sh start nom_instance`
- Pour configurer l'agent à l'aide du fichier de réponses silencieux, procédez comme suit :
  1. Dans un éditeur de texte, ouvrez le fichier `sap_hana_silent_config.txt` disponible dans le chemin d'accès *rép_install*`\samples` et indiquez les valeurs pour tous les paramètres.

     Windows `C:\IBM\APM\samples`

     Linux AIX `/opt/ibm/apm/agent/samples`
  2. Sur la ligne de commande, changez le chemin d'accès au *rép_install* `\casier`
  3. Exécutez la commande suivante :

     Windows `sap_hana_database-agent.bat config nom_instance rép_install\samples\sap_hana_silent_config.txt`

     Linux AIX `sap_hana_database-agent.sh config nom_instance rép_install\samples\sap_hana_silent_config.txt`
  4. Démarrez l'agent.

     Windows Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.

Linux AIX Exécutez la commande suivante : `./sap_hana_database-agent.sh start nom_instance`

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de la surveillance de SAP NetWeaver Java Stack

Vous devez configurer l'Agent SAP NetWeaver Java Stack pour qu'il puisse collecter les données de surveillance des ressources du serveur d'applications SAP NetWeaver surveillé. Pour surveiller les données de diagnostic et de suivi des transactions, vous devez effectuer certaines tâches de configuration.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for SAP NetWeaver Java Stack agent

Assurez-vous d'effectuer les tâches prérequises suivantes avant de configurer l'agent :

- Copiez les fichiers JAR suivants dans le répertoire `bin` :
  - `sapj2eeclient.jar` (l'API client SAP J2EE Engine qui inclut l'adaptateur JMX)
  - `logging.jar` (la bibliothèque de journalisation)
  - `com_sap_pj_jmx.jar` (la bibliothèque SAP-JMX)
  - `exception.jar` (l'infrastructure des exceptions SAP)

  Le répertoire `bin` se trouve à l'emplacement suivant :
  candle_home\TMAITM6_x64
  candle_home/*interp*/sv/bin

  Important : Les fichiers JAR sont les mêmes pour tous les systèmes d'exploitation pris en charge. Ces fichiers sont disponibles dans le correctif de l'agent de diagnostic ou le gestionnaire SUM (Software Update Manager).
- Affectez le rôle NWA_READONLY à l'utilisateur *Invité* pour qu'il collecte les données de diagnostic et de suivi des transactions.

Pourquoi et quand exécuter cette tâche

L'Agent SAP NetWeaver Java Stack est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser l'interface graphique ou le fichier de réponses silencieux.
- Pour configurer l'agent sur des systèmes d'exploitation Linux ou AIX, vous pouvez utiliser la ligne de commande ou le fichier de réponses silencieux.

Pour configurer la collecte des données de diagnostic et de suivi des transactions, procédez comme suit :

1. Configurez le collecteur de données. Pour plus d'informations, voir «Configuration du collecteur de données», à la page 704.
2. Activez la collecte des données de suivi des transactions et de diagnostic. Pour plus d'informations, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 705.

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management.

Avant de commencer

Assurez-vous que les fichiers qui sont listés dans la section «Avant de commencer» de la rubrique «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 701 sont disponibles dans le répertoire `bin`.

Pourquoi et quand exécuter cette tâche

L'Agent SAP NetWeaver Java Stack fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis cliquez sur **Configuration de l'agent**. La fenêtre Monitoring Agent for SAP NetWeaver Java Stack s'affiche.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système à 3 chiffres du système SAP NetWeaver Java Stack. Par exemple, si l'identificateur système (SID) du système géré SAP NetWeaver Java Stack est P14, entrez `P14` comme nom d'instance.
4. Dans la fenêtre Monitoring Agent for SAP NetWeaver Java Stack, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 708.
5. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance des ressources collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir Démarrage de la console Performance Management.
- Pour collecter les données de diagnostic et de suivi des transactions, configurez le collecteur de données et activez la collecte de données de diagnostic et de suivi des transactions.

Configuration de l'agent sur des systèmes Linux ou AIX

Pour configurer l'agent sur les systèmes Linux ou AIX, vous devez exécuter le script et répondre aux invites.

Avant de commencer

Assurez-vous que les fichiers qui sont mentionnés dans la section «Avant de commencer» de la «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 701 sont disponibles dans le répertoire `bin`.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent.

   Linux `/opt/ibm/apm/agent/bin`

   Linux AIX `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante :

   `./sap_netweaver_java_stack-agent.sh config nom_instance`

   où *nom_instance* est le nom à attribuer à l'instance.

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système à 3 chiffres du système SAP NetWeaver Java Stack. Par exemple, si l'identificateur système (SID) du système géré SAP NetWeaver Java Stack est P14, entrez `P14` comme nom d'instance.
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez sur Entrée :

   `Edit 'Monitoring Agent for SAP NetWeaver Java Stack' setting? [1=Yes, 2=No]`
4. A l'invite, indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 708.
5. Exécutez la commande suivante pour démarrer l'agent :

   `./sap_netweaver_java_stack-agent.sh start nom_instance`

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance des ressources collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir Démarrage de la console Performance Management.
- Pour collecter les données de diagnostic et de suivi des transactions, configurez le collecteur de données et activez la collecte des données de diagnostic et de suivi des transactions.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Avant de commencer

Assurez-vous que les fichiers qui sont mentionnés dans la section «Avant de commencer» de la «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 701 sont disponibles dans le répertoire `bin`.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `sap_netweaver_java_stack_silent_config.txt` disponible dans le chemin d'accès suivant et indiquez les valeurs pour les paramètres de configuration.

   Windows

Windows C:\IBM\APM\samples

Linux AIX /opt/ibm/apm/agent/samples

Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 708.

2. Sur la ligne de commande, changez le chemin d'accès au rép_install\bin.
3. Exécutez la commande suivante :

   Windows sap_netweaver_java_stack-agent.bat config *nom_instance* rép_install\samples\sap_netweaver_java_stack_silent_config.txt

   Linux AIX ./sap_netweaver_java_stack-agent.sh config *nom_instance* rép_install\samples\sap_netweaver_java_stack_silent_config.txt
4. Démarrez l'agent.

   Windows Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent que vous avez créée, puis cliquez sur **Démarrer**. Sinon, vous pouvez également exécuter la commande suivante : sap_netweaver_java_stack-agent.bat start *nom_instance*

   Linux AIX Exécutez la commande suivante : ./sap_netweaver_java_stack-agent.sh start *nom_instance*

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance des ressources collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir Démarrage de la console Performance Management.
- Pour collecter les données de diagnostic et de suivi des transactions, configurez le collecteur de données et activez la collecte des données de diagnostic et de suivi des transactions.

Configuration du collecteur de données

Vous pouvez configurer le collecteur de données pour chaque instance du serveur d'applications que vous voulez surveiller.

Avant de commencer

Assurez-vous que les fichiers qui sont mentionnés dans la section «Avant de commencer» de la «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 701 sont disponibles dans le répertoire bin.

Procédure

Pour configurer le collecteur de données en répondant à des invites, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire Windows rép_install\svdchome*n° de version*\bin\configNW ou Linux AIX rép_install/svdchome/*n° de version*/bin/configNW et exécutez le script suivant :

   Windows config.bat

   Linux AIX config.sh
2. Sélectionnez la version de NetWeaver Server en saisissant le numéro qui correspond au produit pour lequel vous voulez configurer le collecteur de données et appuyez sur Entrée.
3. Lorsque vous êtes invité à indiquer le nom d'utilisateur, entrez celui qui est configuré sur SAP NetWeaver Application Server with Java Stack, et appuyez sur Entrée.
4. Lorsque vous êtes invité à indiquer un mot de passe, entrez le mot de passe, puis appuyez sur Entrée.
5. Lorsque vous êtes invité à entrer à nouveau le mot de passe, entrez-le à nouveau, puis appuyez sur Entrée.

6. Lorsque vous êtes invité à indiquer un numéro de port P4, entrez le numéro de port P4 de l'instance de SAP NetWeaver Application Server disponible sur l'ordinateur local, puis appuyez sur Entrée.

   Important : Utilisez cette formule pour calculer le numéro de port P4 : 50000 + (instance number*100) + 4
7. Lorsque vous êtes invité à sélectionner le numéro d'instance de NetWeaver Server, entrez le numéro qui correspond à l'instance que vous souhaitez configurer, puis appuyez sur Entrée.

   A faire : Vous devez, pour chaque instance, configurer le collecteur de données séparément.
8. A l'invite, entrez 1 si vous souhaitez activer la collecte des données de suivi des transactions. Sinon, entrez 2 et appuyez sur Entrée.
9. A l'invite, entrez 1 si vous souhaitez activer la collecte des données de diagnostic. Sinon, entrez 2 et appuyez sur Entrée.

Résultats

Le chemin d'accès est généré pour charger les fichiers classe.

Que faire ensuite

1. Ajoutez le chemin généré à la variable d'environnement appropriée.

   Windows *PATH*

   Linux *LD_LIBRARY_PATH* et *LIBPATH*

   AIX *LD LIBRARY PATH* et *LIB PATH*

   A faire :

   Windows Ajoutez le chemin généré à la variable d'environnement *PATH*.

   Linux Ajoutez le chemin généré aux variables d'environnement *LD_LIBRARY_PATH* et *LIBPATH* dans le fichier `/home/sidadm/.cshrc` au format suivant.

   ```
   setenv LD_LIBRARY_PATH /path

   setenv LIBPATH /path
   ```

   AIX Ajoutez le chemin généré aux variables d'environnement *LD LIBRARY PATH* et *LIB PATH* dans le fichier `/etc/environment` au format suivant.

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/path

   LIBPATH=$LIBPATH:/path
   ```
2. Redémarrez les instances du serveur d'applications.
3. Activez la collecte des données de suivi des transactions et de diagnostic. Pour plus d'informations, voir «Activation de la collecte des données de suivi des transactions et de diagnostic».

Activation de la collecte des données de suivi des transactions et de diagnostic

Sur la page Configuration d'agent, vous pouvez activer ou désactiver la collecte des données de diagnostic ou de suivi des transactions.

Avant de commencer

Vérifiez que le collecteur de données est configuré. Pour plus d'informations, voir «Configuration du collecteur de données», à la page 704.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez la collecte des données de suivi des transactions, l'agent collecte les données des composants suivants :

- Servlet JSP
- RemoteEJB
- JMS

Procédure

Pour configurer la collecte des données pour chaque instance de SAP NetWeaver Application Server, procédez comme suit :

1. Connectez vous à la console Cloud APM.
2. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
3. Cliquez sur l'onglet **NetWeaver**.
4. Cochez les cases des instances de SAP NetWeaver Application Server pour lesquelles vous souhaitez configurer la collecte de données, puis effectuez l'une des actions suivantes de la liste **Actions**.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour activer la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode Only**. Le statut indiqué dans la colonne Diagnostic Mode est mis à jour sur Enabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour activer la collecte des données de diagnostic et la trace de méthode, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes Diagnostic Mode and Method Trace est mis à jour sur Enabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Disabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour désactiver la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Disabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes **Diagnostic Mode and Method Trace** est mis à jour sur Disabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.

Résultats

La collecte de données est configurée pour chaque instance de SAP NetWeaver Application Server sélectionnée.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données de suivi des transactions et de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Suppression de la configuration du collecteur de données

Vous pouvez annuler les modifications effectuées lors de la configuration du collecteur de données pour une instance de SAP Netweaver Application Server with Java Stack.

Procédure

Pour supprimer la configuration du collecteur de données en répondant à des invites, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire Windows `rép_install\svdchome\n° de version\bin\configNW` ou Linux AIX `rép_install/svdchome/n° de version/bin/configNW` et exécutez le script suivant :

   Windows unconfig.bat

   Linux AIX unconfig.sh

   Toutes les instances pour lesquelles le collecteur de données est configuré sont répertoriées.
2. Entrez le numéro qui correspond à l'instance pour laquelle vous voulez supprimer la configuration du collecteur de données et appuyez sur Entrée.

   Conseil : Pour supprimer la configuration du collecteur de données pour plusieurs instances, entrez le numéro qui correspond aux instances séparé par des virgules. Pour supprimer la configuration du collecteur de données pour toutes les instances, vous pouvez exécuter les scripts suivants :

   Windows config.bat -a

   Linux AIX config.sh -a

Que faire ensuite

Redémarrez les instances de SAP NetWeaver AS with Java Stack.

Restauration de l'instance SAP NetWeaver Application Server

Vous pouvez utiliser l'utilitaire de restauration pour restaurer les paramètres JVM si l'instance SAP NetWeaver Application Server ne démarre pas après la configuration de SAP NetWeaver Data Collector, ou pour restaurer l'instance SAP NetWeaver Application Server.

Procédure

Pour restaurer l'instance SAP NetWeaver Application Server en répondant aux invites, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire Windows `rép_install\svdchome\n° de version\bin\configNW` ou Linux AIX `rép_install/svdchome/n° de version/bin/configNW` et exécutez le script suivant :

   Windows `restoreNW.bat`

   Linux AIX `restoreNW.sh`
2. Sélectionnez la version de NetWeaver Server en entrant le numéro qui correspond au produit pour lequel vous souhaitez restaurer les paramètres JVM, puis appuyez sur Entrée.
3. Lorsque vous êtes invité à indiquer le nom d'utilisateur, entrez celui de l'instance SAP NetWeaver Application Server et appuyez sur Entrée.
4. Lorsque vous êtes invité à indiquer le mot de passe utilisateur, entrez celui de l'instance SAP NetWeaver Application Server et appuyez sur Entrée.
5. Lorsque vous êtes invité à indiquer un numéro de port P4, entrez celui de l'instance SAP NetWeaver Application Server disponible sur l'ordinateur local et appuyez sur Entrée.

Si les informations d'instance sont introuvables avec le port P4 indiqué, le message `Could not connect to SAP NetWeaver Server` s'affiche et vous êtes invité à entrer le chemin du répertoire principal de l'instance NetWeaver Server. Par exemple : `usr\sap\`*`nom_système`*`\`*`numéro_instance`*

6. Lorsque vous êtes invité à sélectionner le numéro d'instance NetWeaver Server, entrez le numéro qui correspond à l'instance à restaurer, puis appuyez sur Entrée.

Résultats

Le message suivant s'affiche :

```
Restore successful. Please restart the instance.
```

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent SAP NetWeaver Java Stack, vous pouvez modifier la valeur par défaut des paramètres, comme SAP_NETWEAVER_P4_HOSTNAME et SAP_NETWEAVER_P4_PORT.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'Agent SAP NetWeaver Java Stack. Vous devez indiquer une valeur pour toutes les zones car elles sont obligatoires.

Tableau 165. Noms et descriptions des paramètres de configuration

Nom du paramètre	Description
Nom d'instance	Nom de l'instance. La valeur par défaut de cette zone est identique à celle que vous avez indiquée dans la zone **Enter a unique instance name**.
SAP_NETWEAVER_P4_ HOSTNAME	Nom d'hôte ou adresse IP du serveur SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ PORT	Numéro de port P4 du serveur SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ USERNAME	Nom d'utilisateur de l'administrateur donnant accès au serveur SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ PASSWORD	Mot de passe de l'administrateur donnant accès au serveur SAP NetWeaver Application Server.
Confirm SAP_NETWEAVER_P4_ PASSWORD	Mot de passe spécifié pour le paramètre **SAP_NETWEAVER_P4_PASSWORD**.

Configuration de la surveillance de Siebel

L'agent Siebel permet de surveiller de manière centralisée vos ressources Siebel, notamment les statistiques Siebel, les sessions utilisateur, les composants, les tâches, le serveur d'application, le serveur de noms de passerelle Siebel, l'utilisation de la mémoire et de l'UC de processus et la surveillance des événements du journal.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance de Siebel» pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, voir tableau 166.

Tableau 166. Versions d'agent

Version d'agent	Documentation
1.0.0, 1.0.0.1, 1.0.0.2, 1.0.0.2.1	Cloud APM 8.1.4

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Siebel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Siebel.
- Avant de configurer l'agent Siebel, vous devez vérifier le compte utilisateur Siebel utilisé par l'agent Siebel.

Le paramètre "Per Component Statistics Monitoring" est désactivé par défaut. Vous pouvez activer le paramètre "Per Component Statistics Monitoring".

Pourquoi et quand exécuter cette tâche

L'agent Siebel est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Procédure

1. Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 711.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 716.
2. Pour configurer l'agent sur des systèmes d'exploitation Linux et UNIX, vous pouvez exécuter le script et répondre aux invites ou utiliser le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 715.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 716.

Que faire ensuite

Dans la console Cloud APM, accédez aux pages du Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Vérification du compte utilisateur Siebel

Vous devez vérifier le compte utilisateur qui est utilisé pour exécuter l'agent Siebel avant de configurer l'agent.

Pourquoi et quand exécuter cette tâche

Le compte utilisateur qui est utilisé pour exécuter l'agent Siebel doit disposer de droits lui permettant d'exécuter l'utilitaire de ligne de commande Siebel **srvrmgr**. Pour vérifier que le compte utilisateur dispose des droits requis, procédez comme suit :

Procédure

1. Connectez-vous à l'ordinateur avec le compte utilisateur utilisé pour exécuter l'agent Siebel.
2. Déplacez le répertoire à l'emplacement où le serveur Siebel est installé.
3. Sourcez le fichier d'environnement Siebel : **source siebenv.sh**
4. Exécutez la commande suivante :

   ```
   srvrmgr /s serveur_Siebel /g passerelle_Siebel /e entreprise_Siebel
   /u compte_utilisateur /p mot_de_passe
   /c "list servers"
   ```

   où

   serveur_Siebel
   Nom du serveur d'applications Siebel.

   passerelle_Siebel
   Nom du serveur de noms de passerelle actuellement actif.

   entreprise_Siebel
   Nom de l'entreprise Siebel.

   compte_utilisateur
   Compte utilisateur que vous utilisez pour vous connecter à l'ordinateur.

   mot_de_passe
   Mot de passe associé au compte utilisateur.

   Si le compte utilisateur dispose des droits requis, une sortie similaire à l'exemple suivant indique que le nombre de zones renvoyées est limité à trois :

   ```
   Connected to 1 server(s) out of a total of 1 server(s) in the enterprise

   srvrmgr:s82win8> list servers show SBLSRVR_NAME, HOST_NAME, SBLSRVR_STATUS

   SBLSRVR_NAME  HOST_NAME  SBLSRVR_STATUS
   ------------  ---------  --------------------------------
   s82win8       s82win8    16.0.0.0 [23057] LANG_INDEPENDENT

   1 row returned.
   ```

   Si la commande **srvrmgr** ne s'exécute pas correctement, adressez-vous à l'administrateur Siebel du serveur. Veillez à définir les variables d'environnement Siebel requises pour le compte utilisateur et assurez-vous que le compte utilisateur dispose des droits appropriés lui permettant d'exécuter la commande **srvrmgr**.

Activation du paramètre "Per Component Statistics Monitoring"

Le paramètre "Per Component Statistics Monitoring" est désactivé par défaut. Vous pouvez activer le paramètre "Per Component Statistics Monitoring" à l'aide de la variable d'environnement KUY_ENABLE_COMP_STATS.

Avant de commencer

En raison d'un problème connu lié aux serveurs de Siebel V8.1 et ultérieure, la collecte des statistiques de composant Siebel risque d'avoir un impact négatif sur l'utilisation de la mémoire du serveur de passerelle Siebel. Ce problème est décrit dans la note technique publiée par Oracle nommée «Gateway Service on Siebel 8.1 or 8.2 Might Consume High Memory Consumption: Recovery (ID document 1269177.1)». Cet article fournit un correctif à ce problème, qui est mis en oeuvre sur le serveur Siebel.

Si le paramètre "Per Component Statistic Monitoring" est requis dans l'environnement, appliquez le correctif Oracle aux serveurs de passerelle de Siebel version 8.1 ou ultérieure avant d'activer le paramètre "Per Component Statistics Monitoring".

Pourquoi et quand exécuter cette tâche

Après avoir appliqué le correctif Oracle, procédez comme suit pour activer le paramètre "Per Component Statistics Monitoring" dans l'agent Siebel :

Procédure

1. Accédez au répertoire d'installation de l'agent Siebel :
   - Windows *rép_install*\TMAITM6_x64
   - Linux AIX *rép_install*/config
2. Editez le fichier de configuration de l'agent Siebel de sorte à définir KUY_ENABLE_COMP_STATS sur true.
   - Windows KUYENV_*nom_instance*
   - Linux AIX uy.environment

   où *nom_instance* est le nom d'instance de l'agent Siebel.
3. Redémarrez l'agent.

   Important : Pour que ce paramètre soit défini par défaut pour toutes les nouvelles instances d'agent, définissez KUY_ENABLE_COMP_STATS sur true dans les modèles de fichier de configuration :
   - Windows KUYENV
   - Linux AIX Ce paramètre a déjà été défini par défaut pour les nouvelles instances d'agent en éditant uy.environment à l'étape 2.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Siebel sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Siebel**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple : siebel01.

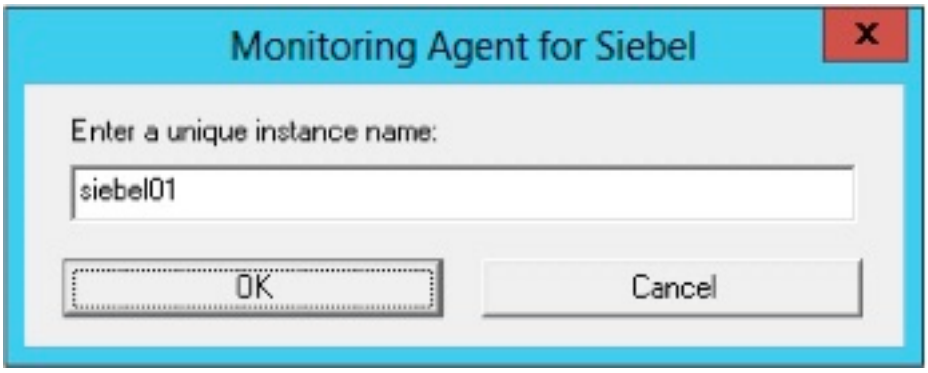


Figure 22. Fenêtre de saisie d'un nom d'instance unique.

4. Sélectionnez un type de serveur et entrez les valeurs appropriées dans les zones obligatoires, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 167, à la page 717.

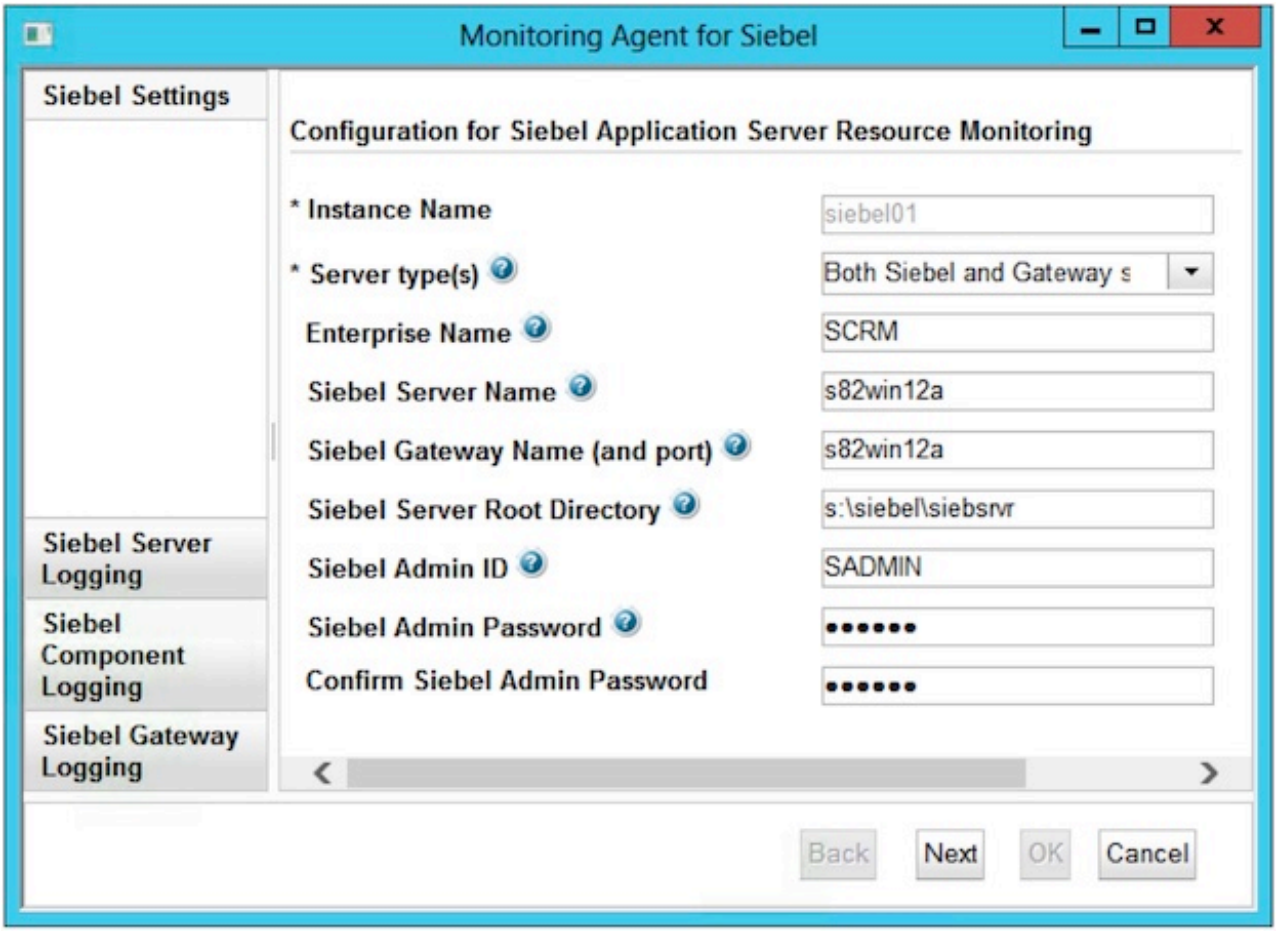


Figure 23. Fenêtre des paramètres de configuration pour les types de serveur Siebel installés sur un hôte Siebel

Important : Si l'agent Siebel est installé sur un ordinateur avec le serveur de noms de passerelle Siebel mais sans le serveur Siebel, les données qui s'affichent dans le Tableau de bord des applications s'appliquent uniquement au serveur de noms de passerelle Siebel pour cette instance. Toutes les autres vues de l'agent Siebel sont vides.

5. Facultatif : Editez les valeurs de consignation du serveur Siebel, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 168, à la page 718.

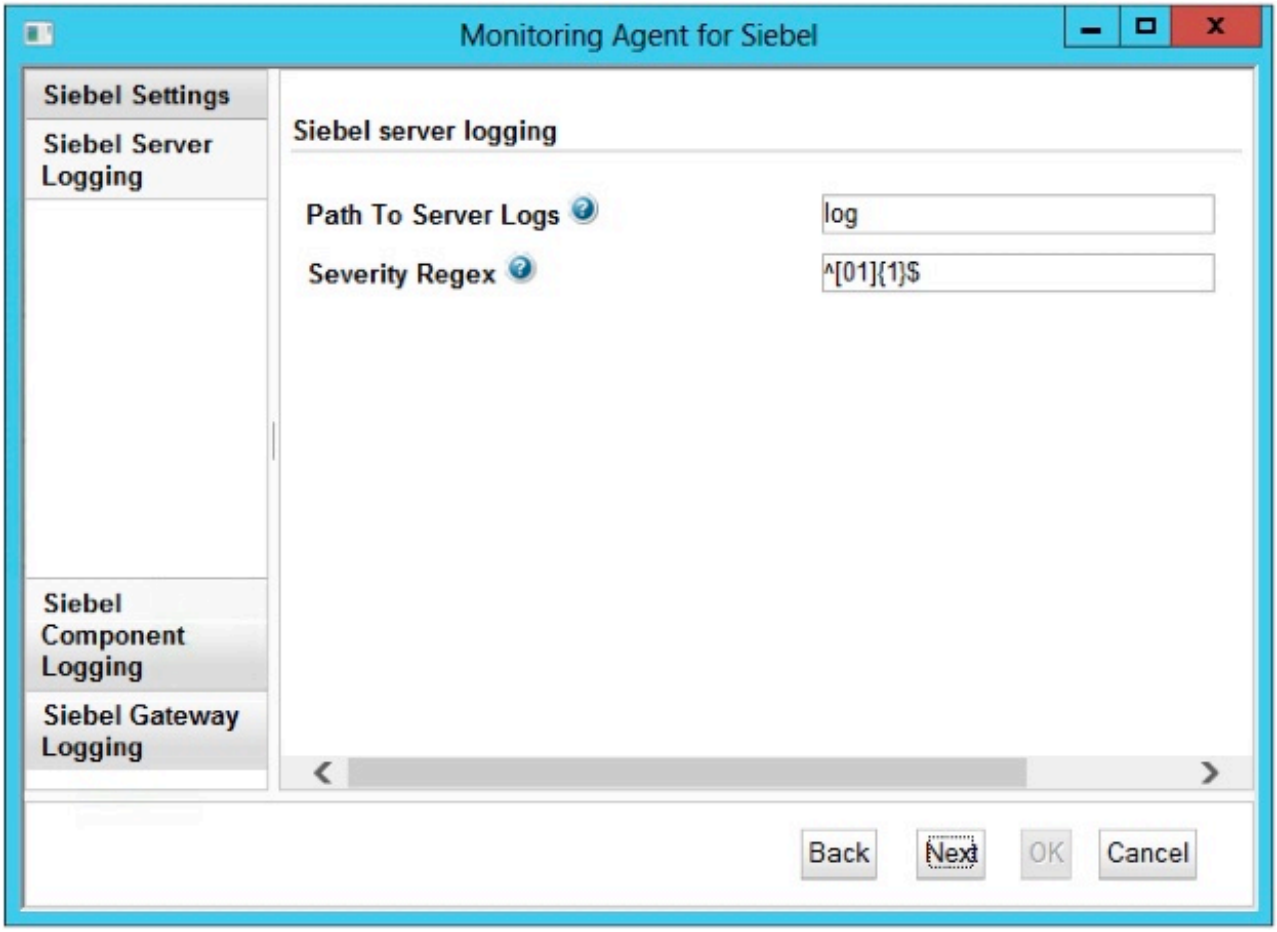


Figure 24. Fenêtre de spécification des paramètres de consignation du serveur Siebel

6. Facultatif : Editez les valeurs de consignation du composant Siebel, puis cliquez sur **Suivant**. Par défaut, les journaux des composants du tableau 171, à la page 719 sont surveillés par l'agent Siebel. Pour ajouter jusqu'à 10 journaux de composant supplémentaires à surveiller, indiquez l'alias de composant correspondant, `SCBroker` par exemple. Pour obtenir une description de chaque paramètre de configuration, voir tableau 169, à la page 718.

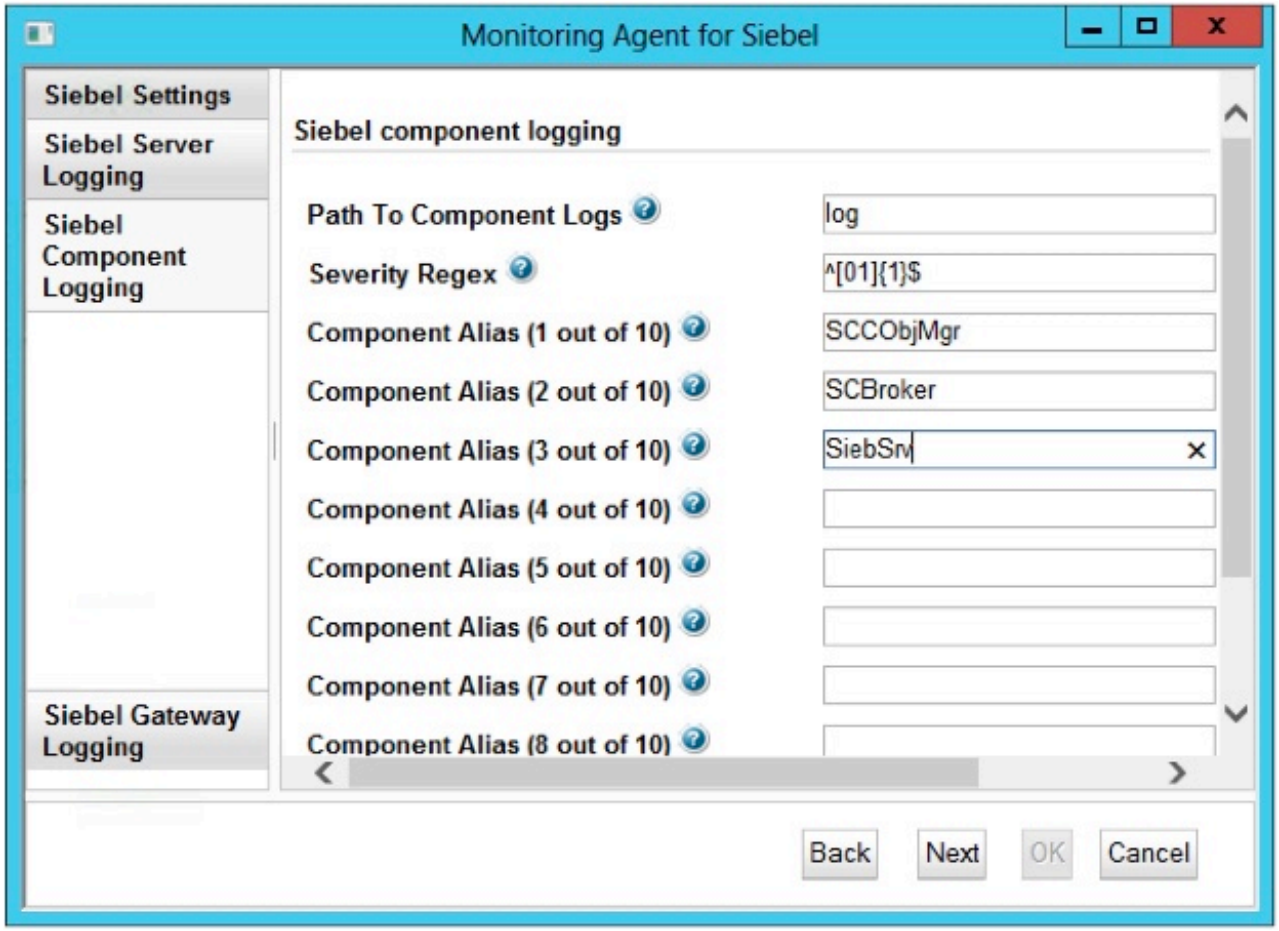


Figure 25. Fenêtre de spécification de journaux de composant supplémentaires à surveiller

7. Facultatif : Editez les valeurs de consignation de la passerelle Siebel. Pour obtenir une description de chaque paramètre de configuration, voir tableau 170, à la page 719.

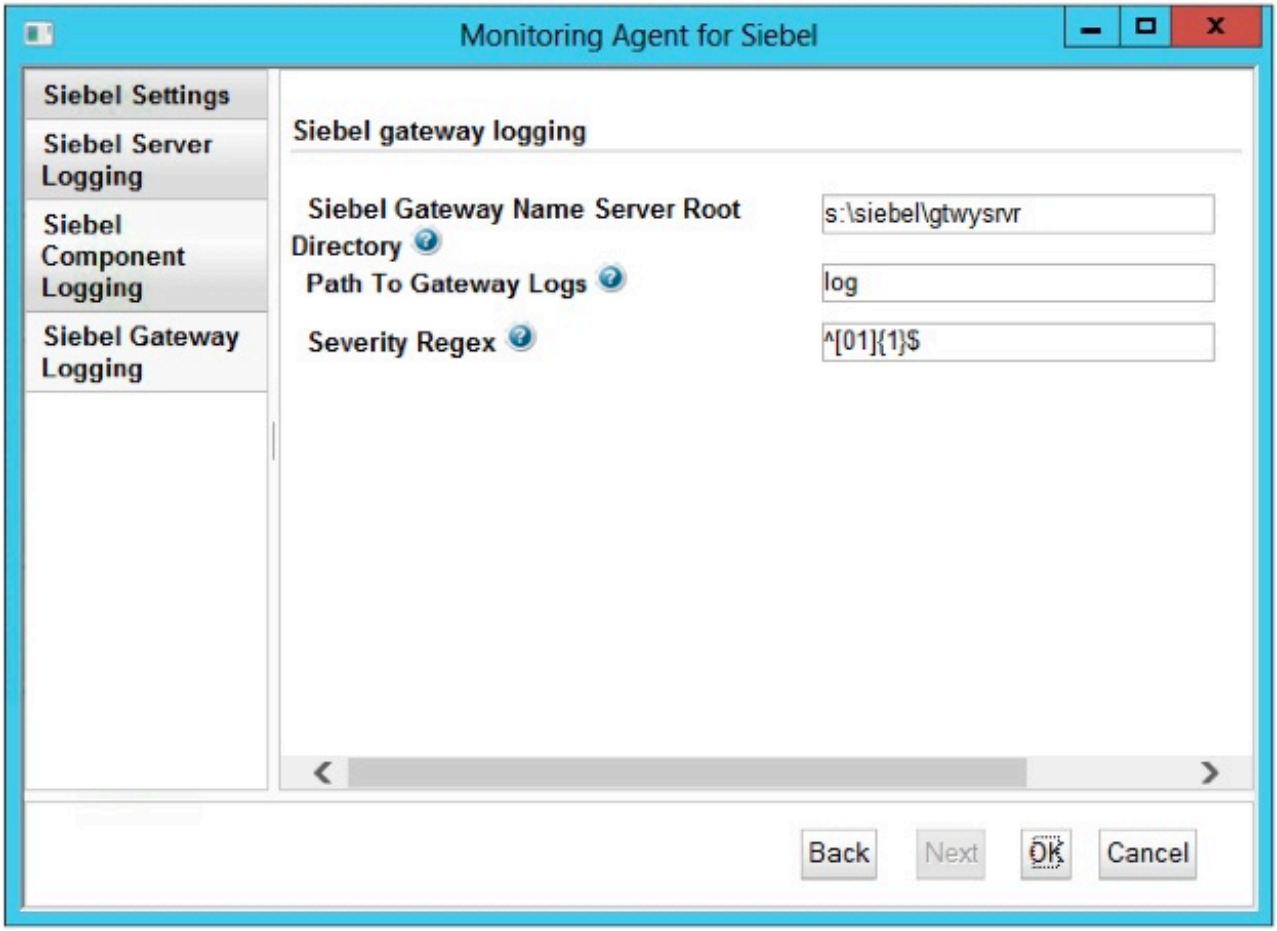


Figure 26. Fenêtre de spécification des paramètres de consignation de la passerelle Siebel

8. Cliquez sur **OK** pour terminer la configuration.
9. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent Siebel, vous devez le configurer pour pouvoir le démarrer. Si l'agent Siebel est installé sur un ordinateur Linux ou UNIX local, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Siebel en exécutant un script et en répondant aux invites.

1. A partir d'une ligne de commande, exécutez la commande suivante :

   rép_install/bin/siebel-agent.sh config **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent. Exemple

```
/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01
```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Siebel», à la page 717.

3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/siebel-agent.sh start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01
   ```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent Siebel en mode silencieux, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier siebel_silent_config.txt disponible à l'emplacement suivant :

   - Linux AIX *rép_install*/samples/siebel_silent_config.txt
   - Windows *rép_install*\samples\siebel_silent_config.txt

   où *rép_install* représente le chemin d'installation de l'agent. Exemple

   - Linux AIX /opt/ibm/apm/agent/samples/siebel_silent_config.txt
   - Windows C:\IBM\APM\samples\siebel_silent_config.txt

2. Dans le fichier siebel_silent_config.txt, indiquez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Siebel», à la page 717.

3. Sauvegardez et fermez le fichier siebel_silent_config.txt et exécutez la commande suivante :

   - Linux AIX *rép_install*/bin/siebel-agent.sh config **nom_instance** *rép_install*/samples/siebel_silent_config.txt
   - Windows *rép_install*\bin\siebel-agent.bat config **nom_instance** *rép_install*\samples\siebel_silent_config.txt

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
   Exemple

- Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/siebel_silent_config.txt`
- Windows `C:\IBM\APM\bin\ siebel-agent.bat config example-inst01 C:\IBM\APM\samples\ siebel_silent_config.txt`

4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux AIX *rép_install*`/bin/siebel-agent.sh start` **`nom_instance`**
   - Windows *rép_install*`\bin\siebel-agent.bat start` **`nom_instance`**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent. Exemple
   - Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01`
   - Windows `C:\IBM\APM\bin\siebel-agent.bat start example-inst01`

Paramètres de configuration de l'agent Siebel

Les paramètres de configuration de l'agent Siebel sont affichés dans des tableaux qui les regroupent par catégories.

1. Paramètres Siebel - Paramètres généraux de l'environnement Siebel.
2. Consignation du serveur Siebel - Paramètres propres à la surveillance des journaux du serveur Siebel.
3. Consignation du composant Siebel - Paramètres propres à la surveillance d'une liste personnalisée de journaux du composant Siebel.
4. Consignation de la passerelle Siebel - Paramètres propres à la surveillance des journaux de la passerelle Siebel.

Tableau 167. Paramètres Siebel

Nom du paramètre	Description	Requis pour la sélection du type de serveur	Nom du paramètre de fichier de configuration en mode silencieux
Server type(s)	Indique les types de serveur installés sur l'ordinateur local.	• **Gateway server only** • **Siebel server only** • **Both Siebel and Gateway server**	**KUY_SERVER_TYPE**
Enterprise Name	Nom de l'entreprise Siebel.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_ENTERPRISE**
Siebel Server Name	Nom du serveur Siebel à surveiller. **Remarque :** Il ne s'agit pas du nom d'hôte du serveur, mais du nom de serveur utilisé lorsque vous exécutez la commande Siebel **`srvrmgr`**.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_SERVER**
Siebel Gateway Name	Serveur de noms de passerelle Siebel à surveiller et éventuellement le port, par exemple, `gtwysrvr` ou `gtwysrvr:1234`.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_GATEWAY**
Siebel Server Root Directory	Répertoire d'installation de base du serveur d'applications Siebel.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_INSTALL_ROOT**

Tableau 167. Paramètres Siebel (suite)

Nom du paramètre	Description	Requis pour la sélection du type de serveur	Nom du paramètre de fichier de configuration en mode silencieux
Siebel Admin ID	ID utilisateur propre à Siebel utilisé par l'agent pour s'authentifier auprès de l'entreprise Siebel lorsque vous exécutez la commande **srvrmgr**. Par exemple : `SADMIN`	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_ADMIN_ID**
Siebel Admin password	Mot de passe de l'administrateur du serveur Siebel.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_ADMIN_PASSWORD**

Tableau 168. Paramètres de consignation du serveur Siebel

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Path To Server Logs	Chemin d'accès relatif issu de «Siebel Server Root Directory» aux journaux du serveur. Pour désactiver la capture de la consignation de serveur Siebel, entrez un chemin d'accès non valide. Par exemple : `xyz`.	**KUY_SERVER_LOGGING_PATH**
Severity Regex	Expression régulière permettant de capturer les journaux du serveur Siebel correspondant à un niveau de gravité. La valeur par défaut `^[01]{1}$` aide à capturer les erreurs de niveau 0 et 1.	**KUY_SERVER_LOGGING_SEVERITY_REGEX**

Tableau 169. Paramètres de consignation du composant Siebel

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Path To Component Logs	Chemin d'accès relatif issu de «Siebel Server Root Directory» aux journaux du serveur. Pour désactiver la capture de la consignation de serveur Siebel, entrez un chemin d'accès non valide. Par exemple : `xyz`.	**KUY_COMPONENT_LOGGING_PATH**
Severity Regex	Expression régulière permettant de capturer les journaux du serveur Siebel correspondant à un niveau de gravité. La valeur par défaut `^[01]{1}$` aide à capturer les erreurs de niveau 0 et 1.	**KUY_COMPONENT_LOGGING_SEVERITY_REGEX**
Component Alias (*N* out of 10)	Alias de composant pour lequel surveiller le journal d'un composant supplémentaire. Exemple : `SCBroker`. Où *N* indique le nombre de composants facultatifs, entre 1 et 10.	**KUY_CUSTCOMPLOG_00** à **KUY_CUSTCOMPLOG_09**

Tableau 170. Paramètres de consignation de la passerelle Siebel

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Siebel Gateway Name Server Root Directory	Répertoire d'installation de base du serveur de noms de passerelle Siebel.	**KUY_GATEWAY_ROOT**
Path To Gateway Logs	Chemin d'accès relatif issu de "Siebel Gateway Name Server Root Directory" aux journaux de la passerelle. Pour désactiver la capture de la consignation de serveur de noms de passerelle, entrez un chemin d'accès non valide. Par exemple : `xyz`.	**KUY_GW_LOGGING_PATH**
Severity Regex	Expression régulière permettant de capturer les journaux du serveur Siebel correspondant à un niveau de gravité. La valeur par défaut `^[01]{1}$` aide à capturer les erreurs de niveau 0 et 1.	**KUY_GW_LOGGING_SEVERITY_REGEX**

Journaux de composant Siebel toujours surveillés

Les journaux de composant sont toujours surveillés pour 10 composants Siebel.

Tableau 171. Alias et noms des composants Siebel pour lesquels les journaux de composant sont toujours surveillés

Alias du composant	Nom du composant
SCCObjMgr	Call Center Object Manager
SMObjMgr	Marketing Object Manager
SSEObjMgr	Sales Object Manager
CommInboundRcvr	Communications Inbound Receiver
CommOutboundMg	Communications Outbound Manager
CommSessionMgr	Communications Session Manager
WorkMon	Workflow Monitor Agent
WfProcBatchMgr	Workflow Process Batch Manager
WfProcMgr	Workflow Process Manager
SiebSrvr	Siebel Server

Configuration de la surveillance Sterling Connect Direct

Vous devez configurer l'Agent Sterling Connect Direct pour qu'il puisse collecter les données issues des serveurs Connect Direct afin de surveiller les statistiques du transfert de fichiers et la santé des serveurs Connect Direct.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel à la page Software Product Compatibility Reports for Sterling Connect Direct agent

Pourquoi et quand exécuter cette tâche

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.

- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis cliquez sur **Configuration de l'agent**.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Remarque : Limitez la longueur du nom d'instance de l'agent, de préférence entre 7 et 10 caractères.
4. Dans la fenêtre Monitoring Agent for Sterling Connect Direct, sous l'onglet Connect Direct Server Details, spécifiez les valeurs des paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 721.
5. Cliquez sur **Suivant**.
6. Dans l'onglet Java Parameters, conservez les valeurs par défaut et cliquez sur **Suivant**.
7. Dans l'onglet Configuration client de l'interface de programme d'application Java, cliquez sur **OK**.
8. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer** pour démarrer l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur les systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Par exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande : **`/sterling_connect_direct-agent.sh config nom_instance`**.

   Remarque : *nom_instance* est le nom que vous souhaitez attribuer à l'instance d'agent.
3. La ligne de commande affiche le message : `Edit 'Monitoring Agent for Sterling Connect Direct' setting? [1=Yes, 2=No]`.
4. Entrez 1 pour éditer les paramètres.
5. A l'invite, indiquez les valeurs des paramètres de configuration. Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 721.
6. Exécutez la commande suivante pour démarrer l'agent : **`./sterling_connect_direct-agent.sh start nom_instance`**

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Monitoring Agent for Sterling Connect Direct sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de réponses silencieux dans *rép_install*/samples/sterling_connect_direct_silent_config.txt.
2. Entrez le nom du serveur, le nom d'utilisateur, le mot de passe et le répertoire d'installation dans le fichier et sauvegardez-le.
3. Dans l'invite de commande, accédez à *rép_install*/bin et exécutez la commande.

   Linux AIX `./sterling_connect_direct-agent.sh config <nom_instance>` *rép_install*/samples/sterling_connect_direct_silent_config.txt.

   Windows `./sterling_connect_direct-agent.bat config <nom_instance>` *rép_install*/samples/sterling_connect_direct_silent_config.txt.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Pour obtenir de l'aide sur le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'Monitoring Agent for Sterling Connect Direct, vous pouvez définir les valeurs des paramètres de configuration.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'Monitoring Agent for Sterling Connect Direct.

Tableau 172. Noms et descriptions des paramètres de configuration

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	La valeur par défaut de cette zone est identique à celle que vous indiquez dans la zone **Enter a unique instance name**.	Oui

Tableau 172. Noms et descriptions des paramètres de configuration (suite)

Nom du paramètre	Description	Zone obligatoire
Nom du serveur	Nom d'hôte ou IP du serveur Sterling Connect Direct.	Oui
Port du serveur	Port du serveur Sterling Connect Direct. La valeur par défaut pour Sterling Connect Direct est 1363.	Oui
Nom d'utilisateur	Nom d'utilisateur permettant de se connecter au serveur Sterling Connect Direct.	Oui
Mot de passe	Mot de passe permettant de se connecter au serveur Sterling Connect Direct.	Oui
Répertoire de base Java	Chemin d'accès au dossier où Java est installé.	Non
Niveau de trace Java	Niveau de trace utilisé par les fournisseurs Java. La valeur par défaut pour Sterling Connect Direct est Error	Oui
Arguments JVM	Ce paramètre permet d'indiquer une liste facultative d'arguments pour la machine virtuelle Java.	Non
Chemin d'accès aux classes pour les fichiers JAR	Chemin d'accès aux fichiers JAR requis par le fournisseur de données d'interface de programme d'application Java qui ne sont pas inclus avec l'agent.	Non

Configuration de la surveillance Sterling File Gateway

L'Monitoring Agent for Sterling File Gateway surveille l'application IBM Sterling File Gateway à l'aide des API REST business-to-business (B2B) et de la base de données de passerelle de fichiers. Vous devez configurer l'Agent Sterling File Gateway pour qu'il puisse collecter les données issues des sources de données et surveiller les statistiques et la santé de l'application Sterling File Gateway. Vous pouvez configurer l'agent sur les systèmes Windows et Linux.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel à la page Software Product Compatibility Reports for Sterling File Gateway agent
- Vérifiez que les API REST B2B sont installées sur votre noeud de passerelle de fichiers. Pour plus d'informations sur l'installation de l'API REST B2B, voir «Installation de l'API REST B2B».

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Installation de l'API REST B2B

Vous pouvez installer et configurer les API REST business-to-business (B2B) sur votre noeud Sterling File Gateway. Les API REST B2B sont disponibles dans le programme d'installation de B2B Integrator (V5.2.6.2).

Procédure

1. Accédez au répertoire `<rép_install>/bin`.

   Où *rép_install* est le répertoire du programme d'installation de l'agent pour B2B Integrator.
2. Exécutez la commande suivante :

- Linux `./InstallService.sh/rép_install/bin/b2bAPIs_10000602.jar`
  Où <*rép_install*> est l'emplacement d'extraction du contenu du fichier de support.
- Windows `./InstallService.cmd/rép_install/bin/b2bAPIs_10000602.jar`
  Où <*rép_install*> est le dossier du programme d'installation de B2B.

Configuration de l'Agent Sterling File Gateway sur des systèmes Windows

Vous pouvez configurer l'Agent Sterling File Gateway sur des systèmes d'exploitation Windows à l'aide de la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Sterling File Gateway**, puis sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** n'est pas disponible. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Agent Sterling File Gateway, procédez comme suit :
   a. Entrez un nom unique pour l'instance d'Agent Sterling File Gateway et cliquez sur **OK**.
   b. Dans l'onglet relatif aux **détails d'API B2B**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   c. Dans l'onglet relatif aux **détails de base de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   d. Dans l'onglet relatif à l'**API Java**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Agent Sterling File Gateway, consultez les rubriques suivantes :
   - «Paramètres de configuration des détails de l'API B2B», à la page 727
   - «Paramètres de configuration des détails de la base de données», à la page 728
   - «Paramètres de configuration de l'API Java», à la page 728
4. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Agent Sterling File Gateway**, puis sur **Démarrer**.

Configuration de l'Agent Sterling File Gateway sur les systèmes Linux

Vous pouvez exécuter le script de configuration et répondre aux invites pour configurer l'Agent Sterling File Gateway sur les systèmes d'exploitation Linux.

Procédure

1. Accédez à la ligne de commande et exécutez la commande **<rép_install>/bin/sterling_file_gateway-agent.sh config nom_instance**.

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le chemin d'accès au répertoire d'installation de l'agent.

2. Vous êtes invité à saisir des valeurs pour tous les paramètres de configuration obligatoires. Vous pouvez modifier les valeurs par défaut des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :

   - «Paramètres de configuration des détails de l'API B2B», à la page 727
   - «Paramètres de configuration des détails de la base de données», à la page 728
   - «Paramètres de configuration de l'API Java», à la page 728
3. Pour démarrer l'agent, exécutez la commande **<rép_install>/bin/sterling_file_gateway-agent.sh start nom_instance**.

Configuration de l'Agent Sterling File Gateway à l'aide du fichier de réponses silencieux

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent Sterling File Gateway sans répondre aux invites quand vous exécutez le script de configuration. Vous pouvez configurer l'agent qui utilise le fichier de réponses silencieux sur les systèmes Windows et Linux. Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'Agent Sterling File Gateway en mode silencieux, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier `sterling_file_gatway_silent_config.txt` disponible à l'emplacement suivant :
   - Linux *rép_install*`/samples/sterling_file_gatway_silent_config.txt`

     Par exemple : **/opt/ibm/apm/agent/samples/sterling_file_gateway_silent_config.txt**
   - Windows *rép_install*`\samples\sterling_file_gateway_silent_config.txt`

     Par exemple : **C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**
2. Dans le fichier `sterling_file_gateway_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :

   - «Paramètres de configuration des détails de l'API B2B», à la page 727
   - «Paramètres de configuration des détails de la base de données», à la page 728
   - «Paramètres de configuration de l'API Java», à la page 728
3. Sauvegardez et fermez le fichier `sterling_file_gateway_silent_config.txt` et exécutez la commande suivante :
   - Linux *rép_install*`/bin/sterling_file_gateway-agent.sh config` *nom_instance* *rép_install*`/samples/sterling_file_gateway_silent_config.txt`

     Par exemple : **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh config nom_instance /opt/ibm/apm/agent/samples/sterling_file_gateway_silent_config.txt**

- Windows *rép_install*/bin/sterling_file_gateway-agent.bat config *nom_instance* *rép_install*/samples/sterling_file_gateway_silent_config.txt

  Par exemple : **C:\IBM\APM\bin\sterling_file_gateway-agent.bat config nom_instance C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**

  Où *nom_instance* est le nom à attribuer à l'instance et *rép_install* est le chemin d'accès au répertoire d'installation de l'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*/bin/sterling_file_gateway-agent.sh start *nom_instance*

     Par exemple : **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh start nom_instance**
   - Windows *rép_install*\bin\sterling_file_gateway-agent.bat start *nom_instance*

     Par exemple : **C:\IBM\APM\bin\sterling_file_gateway-agent.bat start nom_instance**

Configuration de variables d'environnement d'agent pour le fournisseur de données sous Linux

Vous pouvez configurer les variables d'environnement de l'Agent Sterling File Gateway pour le fournisseur de données sur les systèmes d'exploitation Linux.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway fournit des variables d'environnement que vous pouvez configurer pour le fournisseur de données.

Procédure

1. Accédez au répertoire <rép_install>/agent/config.
2. Ouvrez le fichier .fg.environment dans un éditeur et éditez les variables d'environnement.

   Pour plus d'informations sur les variables d'environnement d'agent que vous pouvez configurer, voir «Variables d'environnement du fournisseur de données», à la page 726.

Configuration de variables d'environnement d'agent pour le fournisseur de données sous Windows

Vous pouvez configurer les variables d'environnement de l'Agent Sterling File Gateway pour le fournisseur de données sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway fournit des variables d'environnement que vous pouvez configurer pour le fournisseur de données.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent et cliquez sur **Advanced** > **Edit ENV File**, puis éditez les valeurs par défaut des variables d'environnement.

   Pour plus d'informations sur les variables d'environnement d'agent que vous pouvez configurer, voir «Variables d'environnement du fournisseur de données», à la page 726.

Variables d'environnement du fournisseur de données

Après avoir configuré l'Agent Sterling File Gateway, vous pouvez modifier certaines valeurs de durée de seuil relatives à la collecte de données de l'agent. Vous pouvez spécifier ces valeurs dans le fichier d'environnement de l'agent.

Le tableau ci-après contient une description détaillée des variables d'environnement du fournisseur de données.

Tableau 173. Nom et description des variables d'environnement du fournisseur de données

Nom du paramètre	Description
Durée de collecte pour le transfert des fichiers (en heures) (**KFG_FILE_ARRIVED_INTERVAL**)	Durée en heures pendant laquelle l'agent collecte les données pour les transferts de fichiers. La valeur par défaut est 24 heures.
Intervalles de collecte pour les activités de transfert de fichiers qui s'affichent sous forme d'un graphique à courbes (en heures) (**KFG_FILE_ACTIVITY_INTERVAL**)	Durée en heures pendant laquelle l'agent collecte les données pour les activités de transfert de fichiers. La valeur par défaut est 1 heure. Par exemple, l'agent collecte les activités de transfert de fichiers qui se sont produites pendant la dernière heure. Ces données sont visibles sous forme de graphiques à courbes sur la page de l'instance. La valeur par défaut est 1 heure.
Intervalle de seuil des partenaires inactifs (en jours) (**KFG_INACTIVE_PARTNERS_INTERVAL**)	Durée de seuil pendant laquelle le partenaire est inactif ou pendant laquelle il n'a ni reçu ni transféré de fichier. La valeur par défaut est 10 jours. Par exemple, si un partenaire n'a ni reçu ni transféré de fichier ces 10 derniers jours, il apparaît comme «Inactive» sur l'agent.
Nombre maximal de fichiers journaux du fournisseur de données (**KFG_LOG_FILE_MAX_COUNT**)	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.
Taille maximale en ko de chaque journal du fournisseur de données (**KFG_LOG_FILE_MAX_SIZE**)	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.

Tableau 173. Nom et description des variables d'environnement du fournisseur de données (suite)

Nom du paramètre	Description
Niveau de détail dans le journal du fournisseur de données (**KFG_LOG_LEVEL**)	Niveau des détails inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 (Off) : aucun message n'est consigné. • 2 (Severe) : seules les erreurs sont consignées. • 3 (Warning) : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 (Info) : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 (Fine) : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 (Finer) : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 (Finest) : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Si vous sélectionnez cette option, cela risque d'affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 (All) : toutes les erreurs et tous les messages sont consignés.
Extraction d'événements pour tous les transferts de fichiers (**KFG_ALL_FGEVENTS**)	Indicateur d'extraction des événements pour tous les transferts de fichiers. Les valeurs admises sont `Yes` ou `No`. La valeur par défaut est `No`. Si la valeur est définie sur `No`, l'agent extrait les événements associés aux transferts de fichiers ayant échoué pour une durée configurable par l'utilisateur. Si la valeur est définie sur `Yes`, l'agent extrait les événements associés à tous les transferts de fichiers pour une durée configurable par l'utilisateur.

Paramètres de configuration des détails de l'API B2B

Lorsque vous configurez l'Agent Sterling File Gateway, vous devez spécifier les valeurs des paramètres de configuration pour les détails de l'API business-to-business (B2B).

Le tableau ci-après contient une description détaillée des paramètres de configuration des détails de l'API B2B.

Tableau 174. Nom et description des paramètres de configuration des détails de l'API B2B

Nom du paramètre	Description
Nom de l'instance (**KFG_Instance_Name**)	Nom de l'instance. **Restriction :** La zone Nom d'instance contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.
Nom du serveur (**KFG_API_SERVICES_Node_ADDRESS**)	Nom d'hôte ou adresse IP du service d'API B2B.

Tableau 174. Nom et description des paramètres de configuration des détails de l'API B2B (suite)

Nom du paramètre	Description
Port du serveur (**KFG_API_SERVICES_PORT**)	Port de l'API B2B.
Nom d'utilisateur (**KFG_API_SERVICES_USERNAME**)	Nom d'utilisateur permettant de se connecter au service d'API B2B.
Mot de passe (**KFG_API_SERVICES_PASSWORD**)	Mot de passe associé au nom d'utilisateur permettant de se connecter au service d'API B2B.

Paramètres de configuration des détails de la base de données

Lorsque vous configurez l'Agent Sterling File Gateway, vous devez spécifier les valeurs des paramètres de configuration pour les détails de la base de données.

Le tableau ci-après contient une description détaillée des paramètres de configuration des détails de la base de données.

Tableau 175. Nom et description des paramètres de configuration des détails de la base de données

Nom du paramètre	Description
Nom du serveur de base de données (**KFG_DB_Node_ADDRESS**)	Nom d'hôte ou adresse IP du serveur de base de données Sterling File Gateway.
Utilisateur de la base de données (**KFG_DB_USERNAME**)	Nom de l'utilisateur de la base de données.
Mot de passe de la base de données (**KFG_DB_PASSWORD**)	Mot de passe de la base de données.
Port de la base de données (**KFG_DB_PORT**)	Port de la base de données.
Type de base de données (**KFG_DB_TYPE**)	Type de la base de données.

Paramètres de configuration de l'API Java

Lorsque vous configurez l'Agent Sterling File Gateway, vous devez spécifier les valeurs des paramètres de configuration pour l'API Java.

Le tableau ci-après contient une description détaillée des paramètres de configuration de l'API Java.

Tableau 176. Nom et description des paramètres de configuration de l'API Java

Nom du paramètre	Description
Chemin d'accès aux classes pour le fichier JAR externe (**KFG_CLASSPATH**)	Chemin d'accès au fichier JAR du pilote de base de données que vous voulez spécifier pour la base de données correspondante.

Configuration de la surveillance de Sybase Server

L'agent Sybase offre un point central de gestion des bases de données réparties. Il collecte les informations requises pour que les administrateurs de base de données et système puissent examiner les performances du système Sybase Server, détecter rapidement les problèmes et les empêcher. Les administrateurs de base de données et système peuvent définir les options et seuils requis pour déclencher des alertes lorsque le système atteint ces seuils.
Vous devez configurer l'Monitoring Agent for Sybase Server pour surveiller le serveur Sybase.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Sybase.

Pourquoi et quand exécuter cette tâche

L'agent Sybase est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Procédure

1. Configurez l'agent de surveillance.
   - «Configuration de l'agent à l'aide de l'interface de ligne de commande», à la page 730
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 732
2. Démarrez et arrêtez l'agent de surveillance à l'aide de la commande d'agent **sybase-agent**.

   Pour plus d'informations sur la commande **sybase-agent**, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.
3. Connectez l'agent de surveillance au serveur Performance Management à l'aide de la commande **agent2server**.

   Pour plus d'informations sur la commande **agent2server**, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Octroi de droits d'accès

Vous devez octroyer des droits à l'ID utilisateur utilisé pour surveiller le serveur Sybase.

Avant de commencer

Installez l'agent Sybase.

Vous devez disposer du rôle d'administrateur de base de données pour accorder des droits.

Pourquoi et quand exécuter cette tâche

L'ID utilisateur utilisé par l'agent de surveillance doit avoir accès aux tables Sybase et aux tables de surveillance installées.

Vous pouvez effectuer les tâches suivantes :

- Créer un ID utilisateur pour l'agent de surveillance.
- Octroyer des droits au nouvel ID utilisateur et aux tables de surveillance installées.

Si vous n'exécutez pas l'agent Sybase en tant qu'utilisateur `root`, assurez-vous que votre ID utilisateur appartient au groupe `Sybase` et qu'il possède un accès en lecture aux fichiers journaux Sybase.

Procédure

1. Entrez la commande correspondant au système d'exploitation que vous utilisez.
   - Windows

     `cd` *`rép_install`*`\tmaitm6\SQLLIB`
   - UNIX

     `cd` *`rép_install`*`/misc`

   Où *rép_install* représente le répertoire de base dans lequel le serveur Sybase est installé.
2. Utilisez la commande **isql** pour vous connecter au serveur Sybase en tant qu'utilisateur `sa`.

3. Exécutez la commande suivante pour configurer l'ID utilisé par l'agent Sybase pour communiquer avec le serveur Sybase :

   ```
   1>sp_addlogin nom_utilisateur, mdp 2>g
   ```

   Où :

   - *nom_utilisateur* représente l'ID utilisateur. Par défaut, il s'agit de `tivoli`.

     Si l'ID utilisateur n'est pas `tivoli`, éditez le fichier `koygrant.sql` et remplacez `tivoli` par l'ID utilisateur approprié.
   - *mdp* représente le mot de passe de l'utilisateur.

   Remarque :

   Emplacement du fichier `koygrant.sql` :

   - Windows `\opt\ibm\apm\agent\misc\`
   - UNIX `/opt/ibm/apm/agent/misc/`
4. Exécutez la commande suivante pour octroyer des droits aux tables de la base de données :

   ```
   isql -U sa -P mdp -S nomserveur -i chemin_fichier_koygrantkoygrant.sql
   ```

   Où :

   - *mdp* représente le mot de passe de l'utilisateur `sa`.
   - *nomserveur* représente le nom du serveur de base de données.
   - *chemin_fichier_koygrant* correspond à l'emplacement suivant :

     Remarque :
     - Windows `\opt\ibm\apm\agent\misc\`
     - UNIX `/opt/ibm/apm/agent/misc/`
5. Exécutez la commande suivante pour créer les tables proxy utilisées pour les tables de surveillance installées :

   ```
   isql -U sa -P mdp -S nomserveur
        -i $SYBASE/ASE-12_5/scripts/installmontables
   ```

   Où :

   - *mdp* représente le mot de passe de l'utilisateur `sa`.
   - *nomserveur* représente le nom du serveur de base de données.

Que faire ensuite

Une fois que les droits ont été octroyés, vous pouvez configurer l'agent de surveillance.

Configuration de l'agent à l'aide de l'interface de ligne de commande

Vous pouvez configurer l'Monitoring Agent for Sybase Server à l'aide de l'interface de ligne de commande.

Avant de commencer

L'agent Sybase ne prend pas en charge la configuration à distance. Par conséquent, vous devez vous assurer que le serveur Sybase est installé sur le même hôte que l'agent Sybase.

L'agent Sybase ne prend en charge que Sybase Server versions 15.7 et 16.0.

L'ID utilisateur permettant de se connecter au serveur de base de données est créé.

Pourquoi et quand exécuter cette tâche

L'agent Sybase est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Procédure

1. Exécutez la commande ci-après pour configurer l'agent.
   - Windows

     rép_install\bin\sybase-agent.bat*nom_instance*
   - UNIX

     rép_install/bin/sybase-agent.sh *nom_instance*

   Où :
   - *rép_install* est le répertoire d'installation de l'agent.
   - *nom_instance* représente le nom d'instance du serveur Sybase.
2. Lorsque vous êtes invité à saisir des valeurs pour les paramètres ci-après, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une valeur, puis appuyez sur Entrée.
   a. Pour le paramètre `Home Directory`, entrez le chemin d'accès du répertoire principal du serveur Sybase.
      - Windows

        L'exemple de `Home Directory` est `\opt\sybase`.
      - UNIX

        L'exemple de `Home Directory` est `/opt/sybase`.

   b. Pour le paramètre `ASE Directory`, entrez le chemin d'accès du serveur de base de données ASE.
      - Windows

        L'exemple d'`ASE Directory` est `\opt\sybase\ASE-12_5`.
      - UNIX

        L'exemple d'`ASE Directory` est `/opt/sybase/ASE-12_5`.

   c. Pour le paramètre `Open Client Directory`, entrez l'emplacement d'installation de Sybase Open Client.
      - Windows

        L'exemple d'`Open Client Directory` est `\opt\sap\ocs-16_0`.
      - UNIX

        L'exemple d'`Open Client Directory` est `/opt/sap/ocs-16_0`.

   d. Pour le paramètre `USER ID`, entrez l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

      La valeur `USER ID` par défaut est `tivoli`.

   e. Pour le paramètre `PASSWORD`, entrez le mot de passe de l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

   f. Pour le paramètre `VERSION`, entrez la version du serveur Sybase.

      L'agent Sybase ne prend en charge que Sybase server versions 15.7 et 16.0.

   g. Pour le paramètre `ERROR LOG FILE`, entrez le nom de fichier complet du fichier du journal des erreurs du serveur Sybase.
      - Windows

        L'exemple d'`ERROR LOG FILE` est `\opt\sap\ASE-16_0\install\`*`nomserveur`*`.log`.
      - UNIX

        L'exemple d'`ERROR LOG FILE` est `/opt/sap/ASE-16_0/install/`*`nomserveur`*`.log`.

      Où *nomserveur* correspond au nom du serveur Sybase.

h. Pour le paramètre EXTENDED, entrez le paramètre étendu utilisé par le support pour exclure certaines exécutions de curseur. Appuyez éventuellement sur Entrée sans spécifier de valeurs pour exécuter tous les curseurs.

   Les options du paramètre EXTENDED sont DBD2,DBD15,KOYSEGD.

   - DBD2 exclut l'exécution des curseurs pour les ensembles de données Sybase_Database_Detail et Sybase_Database_Summary.
   - DBD15 exclut l'exécution des curseurs pour l'ensemble de données Sybase_Database_Detail.
   - KOYSEGD exclut l'exécution des curseurs pour l'ensemble de données Sybase_Segment_Detail.

Que faire ensuite

Une fois que la configuration est terminée, vous pouvez démarrer l'agent de surveillance et le connecter au serveur Performance Management.

Pour démarrer l'agent Sybase, utilisez la commande d'agent sybase-agent.

Pour connecter l'agent Sybase au serveur Performance Management, utilisez la commande agent2server.

Pour plus d'informations sur les commandes sybase-agent et agent2server, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Vous pouvez configurer l'Monitoring Agent for Sybase Server à l'aide du fichier de réponses silencieux.

Avant de commencer

L'agent Sybase ne prend pas en charge la configuration à distance. Par conséquent, vous devez vous assurer que le serveur Sybase est installé sur le même hôte que l'agent Sybase.

L'agent Sybase ne prend en charge que Sybase server versions 15.7 et 16.0.

L'ID utilisateur permettant de se connecter au serveur de base de données est créé.

Pourquoi et quand exécuter cette tâche

L'agent Sybase est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Vous devez éditer le fichier de réponses silencieux et exécuter la commande d'agent pour configurer l'agent de surveillance.

Procédure

1. Editez le fichier de réponses silencieux.
   - Windows

     Le fichier de réponses silencieux se trouve à l'emplacement suivant : *rép_install*\samples\sybase_silent_config.txt.
   - UNIX

     Le fichier de réponses silencieux se trouve à l'emplacement suivant : *rép_install*/samples/sybase_silent_config.txt.

   Où *rép_install* représente le répertoire d'installation de l'agent.

   a. Pour le paramètre Home Directory, spécifiez le répertoire principal du serveur Sybase.

- Windows

  L'exemple de Home Directory est \opt\sybase.
- UNIX

  L'exemple de Home Directory est /opt/sybase.

b. Pour le paramètre ASE Directory, spécifiez le chemin d'accès du serveur de base de données ASE.
- Windows

  L'exemple d'ASE Directory est \opt\sybase\ASE-12_5.
- UNIX

  L'exemple d'ASE Directory est /opt/sybase/ASE-12_5.

c. Pour le paramètre Open Client Directory, spécifiez l'emplacement d'installation de Sybase Open Client.
- Windows

  L'exemple d'Open Client Directory est \opt\sap\ocs-16_0.
- UNIX

  L'exemple d'Open Client Directory est /opt/sap/ocs-16_0.

d. Pour le paramètre USER ID, spécifiez l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

   La valeur USER ID par défaut est tivoli.

e. Pour le paramètre PASSWORD, spécifiez le mot de passe de l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

f. Pour le paramètre VERSION, spécifiez la version du serveur Sybase.

   L'agent Sybase ne prend en charge que Sybase server versions 15.7 et 16.0.

g. Pour le paramètre ERROR LOG FILE, spécifiez le nom de fichier complet du fichier du journal des erreurs du serveur Sybase.
- Windows

  L'exemple d'ERROR LOG FILE est \opt\sap\ASE-16_0\install*nomserveur*.log.
- UNIX

  L'exemple d'ERROR LOG FILE est /opt/sap/ASE-16_0/install/*nomserveur*.log.

  Où *nomserveur* correspond au nom du serveur Sybase.

h. Pour le paramètre EXTENDED, spécifiez le paramètre étendu utilisé par le support pour exclure certaines exécutions de curseur. Vous pouvez également ne pas le renseigner pour exécuter tous les curseurs.

   Les options du paramètre EXTENDED sont DBD2,DBD15,KOYSEGD.
- DBD2 exclut l'exécution des curseurs pour les ensembles de données Sybase_Database_Detail et Sybase_Database_Summary.
- DBD15 exclut l'exécution des curseurs pour l'ensemble de données Sybase_Database_Detail.
- KOYSEGD exclut l'exécution des curseurs pour l'ensemble de données Sybase_Segment_Detail.

2. Sauvegardez le fichier de réponses silencieux.
3. Exécutez la commande d'agent ci-après pour configurer l'agent de surveillance.
- Windows

  rép_install\bin\sybase-agent.bat config *nom_instance*
  rép_install\samples\sybase_silent_config.txt
- UNIX

  rép_install/bin/sybase-agent.sh config *nom_instance*
  rép_install/samples/sybase_silent_config.txt

Où :

- *rép_install* est le répertoire d'installation de l'agent.

- *nom_instance* représente le nom du serveur Sybase.

Que faire ensuite

Une fois que la configuration est terminée, vous pouvez démarrer l'agent de surveillance et le connecter au serveur Performance Management.

Pour démarrer l'agent Sybase, utilisez la commande **sybase-agent**.

Pour connecter l'agent Sybase au serveur Performance Management, utilisez la commande **agent2server**.

Pour plus d'informations sur les commandes **sybase-agent** et **agent2server**, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Configuration de la surveillance de Synthetic Playback

Vous devez configurer l'Agent Synthetic Playback pour qu'il puisse collecter les données de disponibilité et de performances des applications Web internes. Ces données sont affichées dans le Tableau de bord d'Application Performance.

Pourquoi et quand exécuter cette tâche

Configurez l'Agent Synthetic Playback en exécutant un script et en répondant à des invites. Démarrez le script et vérifiez qu'il est en cours d'exécution.

Procédure

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :
  1. Entrez *rép_install*/bin/synthetic_playback-agent.sh config où *rép_install* est le répertoire d'installation de l'Agent Synthetic Playback.
  2. A l'invite Edit Monitoring Agent for Synthetic Playback settings, entrez 1 pour continuer.
  3. Lorsque vous êtes invité à entrer un nom de centre de données pour votre point de présence de réexécution, entrez un nom qui identifie l'emplacement de l'agent.

     Important : Sélectionnez un nom décrivant le point de présence de réexécution. Lorsque vous effectuez l'installation de votre agent, vous pouvez sélectionner cet emplacement par nom en tant qu'emplacement de réexécution des transactions synthétiques et afficher les données de transaction à partir de cet emplacement dans le Tableau de bord d'Application Performance.
  4. A l'invite Java parameters, sélectionnez un niveau de trace Java. Appuyez sur Entrée pour choisir le paramètre par défaut ou entrez un nombre compris entre 1 et 8 pour définir un niveau de trace.
  5. A l'invite Class path for external jars, appuyez sur Entrée pour laisser la zone vide ou indiquer l'emplacement d'un fichier JAR externe.
- Pour configurer l'agent à l'aide du fichier de réponses silencieux, procédez comme suit :
  1. Dans un éditeur de texte, ouvrez le fichier synthetic_playback_silent_config.txt disponible à l'emplacement *rép_install*/samples. Par exemple :

     Linux `/opt/ibm/apm/agent/samples`
  2. Dans le fichier synthetic_playback_silent_config.txt, supprimez la mise en commentaire et affectez des valeurs aux propriétés suivantes :
     - Pour LOCATION, définissez ce paramètre sur le nom de votre centre de données ou un nom décrivant où votre agent est installé.
     - Pour JAVA_TRACE_LEVEL, définissez ce paramètre sur l'un des niveaux de trace énumérés, tel que JAVA_TRACE_LEVEL=ERROR.

Sauvegardez le fichier.

3. Sur la ligne de commande, accédez au répertoire *rép_install*/bin.
4. Exécutez la commande suivante pour configurer l'agent en mode silencieux :
   synthetic_playback-agent.sh config *rép_install*/samples/synthetic_playback_silent_config.txt

- Pour démarrer l'Agent Synthetic Playback, entrez : *rép_install*/bin/synthetic_playback-agent.sh start.
- Pour vérifier que l'Agent Synthetic Playback est en cours d'exécution, entrez : *rép_install*/bin/synthetic_playback-agent.sh status. Pour plus d'informations, voir tableau 28, à la page 215.

Que faire ensuite

Pour afficher les performances d'applications Web internes, vous devez créer des transactions synthétiques dans Synthetic Script Manager. Pour plus d'informations, voir «Gestion des transactions et des événements synthétiques», à la page 1058.

Configuration de la surveillance de Tomcat

Vous pouvez configurer l'Monitoring Agent for Tomcat à l'aide des paramètres personnalisés ou par défaut pour surveiller les ressources des serveurs d'applications Tomcat. L'agent peut être configuré sur les systèmes Windows et Linux.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Tomcat.

Pourquoi et quand exécuter cette tâche

L'Agent Tomcat est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 28 caractères, en excluant la longueur de votre nom d'hôte. Par exemple, si vous indiquez TOMCAT2 comme nom d'instance, le nom du système géré est TOMCAT2:hostname:OT. Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Afin d'éviter tout problème de droits lorsque vous configurez l'agent, veillez à utiliser le même ID d'utilisateur superutilisateur ou non superutilisateur que celui utilisé pour installer l'agent. Si vous avez installé votre agent en tant qu'utilisateur sélectionné et que vous voulez le configurer en tant qu'un autre utilisateur, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 219. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez démarrer l'agent en tant qu'un autre utilisateur, voir «Démarrage d'agents en tant qu'utilisateur non superutilisateur», à la page 1039.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 177. Versions d'agent et documentation

Version de l'Agent Tomcat	Documentation
6.4.0.3	IBM Cloud Application Performance Management
6.4.0.2	IBM Performance Management 8.1.3 *

* Le lien ouvre une rubrique Knowledge Center sur site.

Configuration de l'Agent Tomcat avec les paramètres par défaut

Vous pouvez utiliser les paramètres par défaut de l'Agent Tomcat pour surveiller le serveur Tomcat. Il n'est pas nécessaire de fournir des informations de configuration supplémentaires autres que le nom de la nouvelle instance.

Avant de commencer

Pour pouvoir configurer l'agent avec les paramètres par défaut, assurez-vous que les prérequis suivants sont remplis :

- L'agent est installé dans le répertoire par défaut.
- L'URL du service JMX utilise le port 8686.
- Le serveur Tomcat est configuré sans autorisation JMX.

Pourquoi et quand exécuter cette tâche

A faire : Lorsque vous configurez l'agent avec les paramètres par défaut, la collecte des données de suivi et de diagnostic approfondi des transactions n'est pas activée.

Procédure

1. Exécutez la commande suivante :
   Linux `rép_install/bin/tomcat-agent.sh config nom_instance rép_install/samples/tomcat_silent_config.txt`
   Windows `rép_install\bin\tomcat-agent.bat config nom_instance rép_install\samples\tomcat_silent_config.txt` Où

   rép_install
   Répertoire d'installation de l'Agent Tomcat.

   nom_instance
   Est le nom que vous voulez attribuer à l'instance.
2. Exécutez la commande suivante pour démarrer l'agent :
   Linux `rép_install/bin/tomcat-agent.sh start nom_instance`
   Windows `rép_install\bin\tomcat-agent.bat start nom_instance`

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management.

Avant de commencer

Assurez-vous que les prérequis suivants sont respectés :

- Java est installé sur le serveur Tomcat où l'agent est installé.
- JMX Remote est activé pour le serveur Tomcat. Pour plus de détails, voir Enabling JMX Remote.
- Le serveur Tomcat est opérationnel.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent à partir de l'invite de commande. Pour plus de détails, suivez les étapes indiquées dans la rubrique «Configuration de l'Agent Tomcat sur les systèmes Linux», à la page 739 et exécutez les commandes avec l'extension .bat au lieu de .sh. La procédure suivante indique comment configurer l'agent à l'aide du panneau de configuration de l'agent.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Agent de surveillance pour Tomcat**.
3. Cliquez sur **Configuration de l'agent**.

   Avertissement : Si **Configuration de l'agent** n'est pas disponible, cliquez sur **Reconfigurer**.
4. Dans la fenêtre Nom de l'instance, indiquez un nom unique pour l'instance d'Agent Tomcat et cliquez sur **OK**.

   Restriction : Le nom de l'instance ne doit pas dépasser 32 caractères.
5. Dans la zone **SERVER NAME**, entrez un nom unique pour identifier le serveur Tomcat qui est surveillé.
6. Dans la fenêtre Java Parameter Settings, effectuez l'une des actions suivantes :
   - Cliquez sur **Next** pour accepter l'emplacement d'installation par défaut de Java, Le chemin d'installation par défaut est `C:\IBM\APM\java\java80_x64\jre`.
   - Dans la zone **Java Home**, indiquez le chemin d'accès si IBM Java est installé à un autre emplacement.
7. Dans la fenêtre JSR-160-Complaint Server, indiquez les détails des paramètres suivants :
   a. Dans la zone **ID utilisateur JMX**, indiquez l'ID de l'utilisateur utilisé pour se connecter au serveur MBean Tomcat lorsque l'autorisation JMX est activée dans Tomcat.
   b. Dans la zone **Mot de passe JMX**, indiquez le mot de passe de l'utilisateur JMX lorsque l'autorisation JMX est activée dans Tomcat.
   c. Dans la zone **Adresse URL de service JMX**, entrez l'URL utilisée pour se connecter au serveur MBean Tomcat. Le format de l'URL est `service:jmx:rmi:///jndi/rmi://`*`nom_hôte`*`:`*`numéro_port`*`/jmxrmi`. L'adresse URL par défaut est valide lorsque le serveur s'exécute sur l'hôte local et utilise le port 8686 comme port JMX. Vous pouvez modifier le nom d'hôte et le numéro de port dans l'URL en conservant le même format.
   d. Dans la liste **Data Collector Configuration**, sélectionnez Oui si vous souhaitez activer la collecte des données de suivi et d'analyse approfondie des transactions.
8. Dans la fenêtre Monitoring Agent for Tomcat, cliquez avec le bouton droit de la souris sur l'instance de l'Agent Tomcat et cliquez sur **Start**.
9. Si vous activez la collecte des données de suivi et d'analyse approfondie des transactions, redémarrez le serveur Tomcat.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Fourniture de la stratégie de sécurité locale pour l'exécution de l'Monitoring Agent for Tomcat sous Windows en tant qu'utilisateur non-administrateur

Des stratégies de sécurité locales sont disponibles pour permettre à un utilisateur non-administrateur d'exécuter un Monitoring Agent for Tomcat sous Windows.

Pourquoi et quand exécuter cette tâche

La combinaison des deux stratégies de sécurité locales suivantes permet à un utilisateur non-administrateur d'exécuter l'Agent Tomcat sous Windows. Avec ces stratégies, l'utilisateur non-administrateur peut démarrer/arrêter, configurer un Agent Tomcat et en vérifier les données :

1. Déboguer les programmes.
2. Ouvrir une session en tant que service.

Suivez la procédure fournie pour accorder les droits de sécurité locaux à un utilisateur non-administrateur.

Procédure

1. Accédez à TEMA et définissez les paramètres de démarrage de l'agent Tomcat pour un utilisateur non-administrateur.
2. Ajoutez l'utilisateur non-administrateur sous le dossier d'installation de l'agent Tomcat et accordez des droits complets à ce dossier.
3. Ajoutez l'utilisateur non-administrateur sous la clé de Registre HKEY_LOCAL_MACHINE et cliquez sur **Droits complets**.
4. Exécutez la commande **`secpol.msc`** dans le **menu Démarrer** pour ouvrir les stratégies de sécurité locales.
5. Ensuite, pour ajouter un utilisateur non-administrateur dans les stratégies, reportez-vous à «Droits de la stratégie de sécurité locale».
6. Redémarrez l'agent Tomcat.
7. Vérifiez le statut des agents Tomcat ainsi que les données sur le portail APM.

Droits de la stratégie de sécurité locale

Octroi du droit Déboguer les programmes :
Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, suivez la procédure relative à l'Agent Tomcat décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre Propriétés de Déboguer les programmes apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Octroi du droit Ouvrir une session en tant que service :
Pourquoi et quand exécuter cette tâche

Pour accorder le droit Ouvrir une session en tant que service, suivez la procédure relative à l'Agent Tomcat décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre Stratégie de sécurité locale s'affiche.
2. Dans le panneau de gauche, développez Stratégies locales, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur apparaît dans le panneau de droite.
3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre Propriétés de Ouvrir une session en tant que service apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre Sélectionner des utilisateurs ou des groupes apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Configuration de l'Agent Tomcat sur les systèmes Linux

Exécutez le script de configuration et répondez aux invites pour configurer l'Agent Tomcat sur les systèmes Linux.

Avant de commencer

- JMX Remote est activé pour le serveur Tomcat. Pour plus de détails, voir Enabling JMX Remote.
- Le serveur Tomcat est opérationnel.

Procédure

1. Exécutez la commande suivante :
   rép_install/bin/tomcat-agent.sh config *nom_instance*
   Où *nom_instance* est le nom à attribuer à l'instance.
2. Lorsque vous êtes invité à indiquer une valeur pour SERVER, spécifiez un nom unique pour identifier le serveur Tomcat qui est surveillé et appuyez sur la touche Entrée.
3. Lorsque vous êtes invité à indiquer une valeur pour Java home, appuyez sur Entrée pour accepter l'emplacement par défaut dans lequel la machine virtuelle Java est installée. L'emplacement par défaut est /opt/ibm/apm/agent/JRE/lx8266/jre. Si l'agent n'est pas installé dans le répertoire par défaut, spécifiez *rép_install*/JRE/lx8266/jre.
4. Lorsque vous êtes invité à indiquer une valeur pour JMX user ID, spécifiez l'ID de l'utilisateur qui se connecte au serveur MBean Tomcat. Si l'autorisation JMX n'est pas activée, appuyez sur Entrée.
5. Lorsque vous êtes invité à indiquer une valeur pour JMX password, indiquez le mot de passe de l'utilisateur JMX et confirmez-le. Si l'autorisation JMX n'est pas activée, appuyez sur Entrée.
6. Lorsque vous êtes invité à indiquer une valeur pour JMX service URL, appuyez sur Entrée pour accepter l'URL par défaut ou spécifiez une autre adresse URL de service pour vous connecter au serveur MBean Tomcat. Le format de l'URL est service:jmx:rmi:///jndi/rmi://*nom_hôte*:*numéro_port*/jmxrmi. L'adresse URL par défaut est valide lorsque le serveur s'exécute sur l'hôte local et utilise le port 8686 comme port JMX. Vous pouvez modifier le nom d'hôte et le port dans l'URL en conservant le même format.
7. Lorsque vous êtes invité à indiquer une valeur pour Data Collector Configuration, spécifiez 1, puis appuyez sur la touche Entrée pour activer la collecte des données de suivi et d'analyse approfondie des transactions.
8. Exécutez la commande suivante pour démarrer l'agent :
   rép_install/bin/tomcat-agent.sh start *nom_instance*
9. Si vous activez la collecte des données de suivi et d'analyse approfondie des transactions, redémarrez le serveur Tomcat.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de l'Agent Tomcat à l'aide du fichier de réponses silencieux

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent Tomcat sans répondre aux invites.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `tomcat_silent_config.txt` disponible à l'emplacement suivant :
   rép_install`/samples`
2. Pour le paramètre **KOT_SERVER**, spécifiez un nom unique pour identifier le serveur Tomcat surveillé.
3. Pour le paramètre **Java home**, indiquez le chemin dans lequel la machine virtuelle Java est installée. L'emplacement par défaut est `/opt/ibm/apm/agent/JRE/lx8266/jre`. Si l'agent n'est pas installé dans le répertoire par défaut, spécifiez *rép_install*`/JRE/lx8266/jre`.
4. Pour le paramètre **JMX user ID**, spécifiez l'ID de l'utilisateur qui est utilisé pour se connecter au serveur MBean Tomcat. Vous devez spécifier une valeur pour ce paramètre lorsque l'autorisation JMX est activée dans Tomcat.
5. Pour le paramètre **JMX password**, spécifiez le mot de passe de l'utilisateur JMX. Vous devez spécifier une valeur pour ce paramètre lorsque l'autorisation JMX est activée dans Tomcat.
6. Pour le paramètre **JMX service URL**, spécifiez l'adresse URL de service pour vous connecter au serveur MBean Tomcat. Le format de l'URL est `service:jmx:rmi:///jndi/rmi://`*nom_hôte*`:`*numéro_port*`/jmxrmi`. L'adresse URL par défaut est valide lorsque le serveur s'exécute sur l'hôte local et utilise le port 8686 comme port JMX. Vous pouvez modifier le nom d'hôte et le numéro de port dans l'URL en conservant le même format.
7. Pour le paramètre **KOT_DCCONFIGURATION**, spécifiez `Yes` si vous souhaitez activer la collecte des données de suivi et d'analyse approfondie des transactions.
8. Sauvegardez et fermez le fichier `tomcat_silent_config.txt`, puis exécutez la commande suivante pour mettre à jour les paramètres de configuration de l'agent :
   Linux *rép_install*`/bin/tomcat-agent.sh config` *nom_instance* *rép_install*`/samples/tomcat_silent_config.txt`
   Windows *rép_install*`\bin\tomcat-agent.bat config` *nom_instance* *rép_install*`\samples\tomcat_silent_config.txt`
   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent Tomcat.
9. Exécutez la commande suivante pour démarrer l'agent :
   Linux *rép_install*`/bin/tomcat-agent.sh start` *nom_instance*
   Windows *rép_install*`\bin\tomcat-agent.bat start` *nom_instance*
10. Si vous activez la collecte des données de suivi et d'analyse approfondie des transactions, redémarrez le serveur Tomcat.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Activation de la collecte des données de suivi des transactions et de diagnostic

Sur la page Configuration d'agent, vous pouvez activer ou désactiver la collecte des données de suivi des transactions et de diagnostic.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez la collecte des données de suivi des transactions, l'agent collecte les données des composants suivants :

- Servlet JSP
- Applications EJB
- JMS

Procédure

Procédez comme suit pour configurer la collecte des données pour chaque système géré.

1. Connectez vous à console Cloud APM.
2. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
3. Cliquez sur l'onglet **Tomcat**.
4. Cochez les cases des systèmes gérés pour lesquels vous voulez configurer la collecte de données et effectuez l'une des actions suivantes de la liste **Actions**.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking (Définir le suivi des transactions)** > **Activé**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled pour chaque système géré sélectionné.
   - Pour activer la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode Only**. Le statut indiqué dans la colonne Diagnostic Mode est mis à jour et défini sur Enabled pour chaque système géré sélectionné.
   - Pour activer la collecte des données de diagnostic et la trace de méthode, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes Diagnostic Mode et Method Trace est mis à jour et défini sur Enabled pour chaque système géré sélectionné.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Désactivé**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.
   - Pour désactiver la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Disabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes **Diagnostic Mode et Method Trace** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données de suivi des transactions et de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Configuration de la surveillance de VMware VI

Après avoir installé l'Monitoring Agent for VMware VI, vous devez créer la première instance et démarrer manuellement l'agent pour la collecte des données de l'infrastructure virtuelle VMware en cours de surveillance.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel.
- Créez un ID utilisateur dans votre infrastructure virtuelle VMware. L'agent utilise cet ID utilisateur pour se connecter au vCenter VMware afin de surveiller l'infrastructure virtuelle VMware. Vérifiez que vous disposez des privilèges «System.View» et «System.Read» sur tous les vCenters et serveurs ESX qui sont surveillés. Pour plus d'informations sur la création de l'ID utilisateur, voir les rubriques relatives à la gestion des utilisateurs, des groupes, des droits et des rôles dans la documentation VMware.
- Déterminez si le vCenter est configuré pour la communication SSL. S'il est configuré, alors vous devez configurer Agent VMware VI pour utiliser SSL pour communiquer avec le vCenter.
  - Pour déterminer si le vCenter utilise SSL pour la communication, utilisez l'URL `https://adresseIPvCenter` pour accéder au vCenter. Si vous pouvez accéder au vCenter, alors cela indique que le vCenter utilise SSL pour communiquer sur le réseau.
  - Pour configurer l'Agent VMware VI de façon à ce qu'il utilise SSL pour communiquer avec le vCenter, effectuez les étapes décrites dans la section «Activation de la communication SSL avec les sources de données VMware VI», à la page 743.
- Déterminez le nombre d'instances d'agent dont vous avez besoin pour surveiller votre infrastructure virtuelle VMware. Pour plus d'informations sur la définition du nombre d'instances d'agent conformément à votre environnement de surveillance, voir «Définition de la taille et planification du déploiement de l'Agent VMware VI», à la page 743.

Pourquoi et quand exécuter cette tâche

L'Agent VMware VI est un agent multi-instance. Contrairement à un agent doté d'une seule instance, que vous pouvez configurer pour surveiller et collecter les données pour une seule application surveillée, l'Agent VMware VI peut avoir plusieurs instances configurées qui se connectent à plusieurs serveurs vCenter et surveillent votre infrastructure virtuelle VMware à distance.

Les paramètres de configuration définissent les sources de données de l'infrastructure virtuelle VMware surveillées et établissent une connexion au vCenter VMware, au dispositif serveur vCenter ou à un serveur ESX VMware individuel. Pour connaître les versions prises en charge de ces applications, voir les rapports de compatibilité des produits logiciels pour l'Agent VMware VI.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 178. Versions d'agent et documentation

Version de l'Agent VMware VI	Documentation
7.2.0.8, 7.2.0.9	IBM Performance Management 8.1.4
7.2.0.7, 7.2.0.6	IBM Cloud Application Performance Management

Vous devez configurer manuellement l'agent pour afficher les données de tous les attributs d'agent.

- Pour configurer l'agent sur des systèmes d'exploitation Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes d'exploitation Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Définition de la taille et planification du déploiement de l'Agent VMware VI

Le nombre d'instances d'agent que vous pouvez configurer sur un système unique dépend de la disponibilité et de l'utilisation des ressources sur le système.

Le tableau suivant catégorise l'environnement VMware en fonction de différentes tailles avec la taille de segment de mémoire Java requise :

Tableau 179. Environnement VMware et taille de segment de mémoire Java

Taille de l'environnement VMware	Nombre de serveurs ESX	Taille de segment de mémoire Java
Environnement de petite taille	Un serveur vCenter qui gère jusqu'à 125 serveurs ESX(i) et entre 300 et 1500 invités.	**-Xmx2048m** (2 Go)
Environnement de taille moyenne	Un serveur vCenter qui gère entre 125 et 250 serveurs ESX(i) et entre 1500 et 4000 invités.	**-Xmx4096m** (4 Go)
Environnement de grande taille	Un serveur vCenter qui gère entre 250 et 500 serveurs ESX(i) et entre 4000 et 7500 invités.	**-Xmx8192m** (8 Go)
Environnement de très grande taille	Un serveur vCenter qui gère plus de 500 serveurs ESX(i) et plus de 7500 invités.	**-Xmx16384m** (16 Go)

Pour augmenter la taille de segment de mémoire pour le fournisseur de données Java, effectuez les étapes décrites dans la section «Augmentation de la taille de segment de mémoire Java», à la page 749.

Pour que les instances d'agent surveillent correctement l'environnement, le serveur sur lequel vous installez l'agent doit disposer d'une quantité de ressources de mémoire suffisante pour pouvoir accueillir les données collectées par ces instances d'agent. Une instance unique de l'Agent VMware VI nécessite entre 300 et 400 Mo environ pour surveiller un environnement de petite taille. Reportez-vous aux instructions relatives au nombre d'instances d'agent à configurer :

- Utilisez une instance unique pour surveiller un vCenter unique. N'utilisez pas la même instance pour surveiller plusieurs vCenters.
- Dans un environnement non cluster, utilisez une instance unique pour surveiller un maximum de 8 serveurs ESX de petite taille (entre 100 et 200 machines virtuelles dans un serveur ESX). Ne configurez pas plusieurs serveurs ESX individuels au sein d'une instance d'agent unique.
- Utilisez plusieurs instances de l'Agent VMware VI pour surveiller un environnement contenant plusieurs vCenters. Avant de configurer plusieurs instances, vérifiez que le système sur lequel vous installez l'agent dispose d'une quantité de ressources de mémoire suffisante.

Activation de la communication SSL avec les sources de données VMware VI

Avant de configurer l'agent afin de communiquer de manière sécurisée avec ses sources de données d'infrastructure virtuelle VMware à l'aide de SSL, vous devez ajouter un certificat SSL de source de données au magasin de certificats de confiance de l'agent.

Pourquoi et quand exécuter cette tâche

Important : Les informations ci-dessous ne s'appliquent que si l'agent est configuré de manière à valider les certificats SSL.

Si la validation de certificat SSL est désactivée, l'Agent VMware VI se connecte aux sources de données VMware même si leurs certificats SSL ont expiré, ne sont pas dignes de confiance ou ne sont pas valides. Cependant, la désactivation de la validation des certificats SSL peut poser des problèmes de sécurité et doit être effectuée avec précaution.

Si une source de données VMware utilise un certificat SSL signé par une autorité de certification commune (par exemple Verisign, Entrust ou Thawte), il n'est pas nécessaire d'ajouter des certificats au magasin de clés de confiance de certificats de l'Agent VMware VI. En revanche, si la source de données utilise un certificat qui n'est pas signé par une autorité de certification courante, comme c'est le cas par défaut, vous devez ajouter le certificat au magasin de confiance pour permettre à l'agent de se connecter et de collecter des données.

Remarque :

1. Le fichier de certificat VMware par défaut se nomme `rui.crt`.
2. Pour un centre virtuel, le fichier de certificat SSL se trouve par défaut dans le chemin suivant :
   `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL`
3. Pour un serveur ESX, le fichier du certificat SSL se trouve par défaut dans le répertoire `/etc/vmware/ssl`.

Procédure

1. Copiez le fichier de certificat de votre source de données vers l'ordinateur de l'agent.
2. Sur l'ordinateur de l'agent, placez le fichier de certificat dans le répertoire de votre choix. Evitez tout écrasement des fichiers de certificat. Utilisez un nom de fichier et un libellé uniques pour chaque certificat ajouté.
3. Utilisez la commande *keytool* pour ajouter le certificat de source de données au magasin de clés de confiance de l'agent :

   ```
   keytool -import -noprompt -trustcacerts -alias CertificateAlias -file
   CertificateFile -keystore Truststore -storepass TruststorePassword
   ```

   Où

   CertificateAlias

   Référence unique pour chaque certificat ajouté au magasin de clés de confiance de l'agent ; par exemple, *datasource* est un alias approprié pour le certificat provenant de *datasource.example.com*.

   CertificateFile

   Nom et chemin d'accès complet au fichier de certificat de source de données VMware à ajouter au magasin de clés de confiance.

   Fichier de clés certifiées

   Nom et chemin d'accès complet au fichier de la base de données de certificats de l'Agent VMware VI. Utilisez le chemin et le nom de fichier suivants :

   - Windows (64 bits) : *rép_install*`\tmaitm6_x64\kvm.truststore`
   - Linux (64 bits) : *rép_install*`/lx8266/vm/etc/kvm.truststore`

   TruststorePassword

   ITMVMWAREVI est le mot de passe par défaut du magasin de clés de confiance de l'Agent VMware VI. Pour modifier ce mot de passe, reportez-vous à la documentation relative à l'environnement d'exécution Java pour plus d'informations sur les outils à utiliser.

   Important : Pour utiliser la commande *keytool*, le répertoire bin de l'environnement d'exécution Java doit être indiqué dans le chemin. Utilisez les commandes suivantes :

   - Windows (64 bits) : `set PATH=%PATH%;`*rép_install*`\java\java70_x64\jre\bin`

- Linux (64 bits) : `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`

4. Après avoir ajouté tous les certificats de source de données, démarrez l'agent de surveillance.

Que faire ensuite

Terminez la configuration de l'agent.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre IBM Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'Agent VMware VI fournit les valeurs par défaut de certains paramètres. Vous pouvez indiquer d'autres valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for VMware VI**, puis sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Monitoring Agent for VMware VI, procédez comme suit :
   a. Entrez un nom unique pour l'instance de l'Agent VMware VI et cliquez sur **OK**.
   b. Dans l'onglet **Fournisseur de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   c. Dans l'onglet **Source de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.

      L'Agent VMware VI est un agent applicable à plusieurs sources de données. Vous pouvez surveiller plusieurs sources de données à partir du même agent.
      - Si vous souhaitez configurer une nouvelle source de données, cliquez sur **Nouveau**.
      - Si vous souhaitez supprimer une source de données existante, cliquez sur **Supprimer**.

      Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Monitoring Agent for VMware VI, consultez les rubriques suivantes :
      - Paramètres de configuration du fournisseur de données
      - Paramètres de configuration de la source de données
4. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement VMware de grande taille regroupant plus de 500 hôtes ESX, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 749.

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'Agent VMware VI en mode silencieux, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier `vmware_vi_silent_config.txt` disponible dans l'emplacement suivant :
   - Linux *rép_install*`/samples/vmware_vi_silent_config.txt`
     Exemple : `/opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`
   - Windows *rép_install*`\samples\vmware_vi_silent_config.txt`
     Exemple : `C:\IBM\APM\samples\vmware_vi_silent_config.txt`
2. Dans le fichier `vmware_vi_silent_config.txt`, indiquez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.
   Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données», à la page 748
   - «Paramètres de configuration de la source de données», à la page 747
3. Sauvegardez et fermez le fichier `vmware_vi_silent_config.txt`, puis exécutez la commande suivante :
   - Linux *rép_install*`/bin/vmware_vi-agent.sh config` *nom_instance rép_install*`/samples/vmware_vi_silent_config.txt`
     Exemple : **`/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config nom_instance /opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`**
   - Windows *rép_install*`\bin\vmware_vi-agent.bat config` *nom_instance rép_install*`\samples\vmware_vi_silent_config.txt`
     Exemple : **`C:\IBM\APM\bin\ vmware_vi-agent.bat config nom_instance C:\IBM\APM\samples\vmware_vi_silent_config.txt`**
     Où

     nom_instance
     Nom à attribuer à l'instance.

     rép_install
     Chemin d'installation de l'agent.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
4. Exécutez la commande suivante pour démarrer l'agent :
   - Linux *rép_install*`/bin/vmware_vi-agent.sh start` *nom_instance*
     Exemple : **`/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start nom_instance`**
   - Windows *rép_install*`\bin\vmware_vi-agent.bat start` *nom_instance*

Exemple : **C:\IBM\APM\bin\vmware_vi-agent.bat start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement VMware de grande taille regroupant plus de 500 hôtes ESX, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 749.

Configuration de l'agent en répondant à des invites.

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. A partir d'une ligne de commande, exécutez la commande suivante :

   rép_install/bin/vmware_vi-agent.sh config *nom_instance*

   Exemple : **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config nom_instance**

   Où

   nom_instance
   Nom à attribuer à l'instance.

   rép_install
   Chemin d'installation de l'agent.
2. Répondez aux invites en vous reportant aux rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données», à la page 748
   - «Paramètres de configuration de la source de données»
3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/vmware_vi-agent.sh start *nom_instance*

   Exemple : **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le Forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement VMware de grande taille regroupant plus de 500 hôtes ESX, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 749.

Paramètres de configuration de la source de données

Lorsque vous configurez l'Agent VMware VI, vous pouvez modifier les valeurs par défaut des paramètres de la source de données, comme l'adresse, l'ID utilisateur et le mot de passe de la source de données.

Le tableau ci-après contient une description détaillée des paramètres de configuration de la source de données.

Tableau 180. Noms et descriptions des paramètres de configuration de la source de données

Nom du paramètre	Description	Zone obligatoire
Data Source ID	ID de la source de données.	Oui
Data Source Address	Adresse de la source de données. Si vous ne souhaitez pas que l'agent valide les certificats SSL, définissez une valeur correspondant au nom d'hôte ou à l'adresse IP du centre virtuel VMware ou du serveur ESX surveillé. Si vous souhaitez que l'agent valide les certificats SSL lorsque SSL est utilisé pour communiquer via le réseau, configurez l'agent à l'aide de l'élément Subject Alternative Name fourni dans le certificat. Pour afficher l'élément subject alternative name du centre de données, procédez comme suit : 1. Ouvrez le certificat. 2. Dans la fenêtre **Certificate**, cliquez sur l'onglet **Details**. 3. Sélectionnez **Subject Alternative Name** et utilisez la valeur de DNS Name. Par exemple, si la valeur de DNS Name est «`ibmesx3v3vc.ITMfVS.com`», utilisez la valeur «`ibmesx3v3vc.ITMfVS.com`» pour le nom d'hôte.	Oui
Use SSL Connection to Data Source	Indique si l'agent utilise une connexion SSL pour se connecter aux sources de données de l'infrastructure virtuelle VMware. Indiquez `Yes` si l'agent utilise une connexion SSL pour se connecter aux sources de données. Sinon, indiquez `No`. La valeur par défaut est `Yes`.	Oui
Data Source User ID	ID utilisateur doté de privilèges suffisants pour collecter des données de surveillance et reconnu par la source de données.	Oui
Data Source Password	Mot de passe de l'ID utilisateur configuré pour accéder à la source de données.	Oui
Confirm Data Source Password	Mot de passe correspondant à celui indiqué dans la zone **Data Source Password**.	

Paramètres de configuration du fournisseur de données

Lorsque vous configurez l'Agent VMware VI, vous pouvez modifier les valeurs par défaut des paramètres pour le fournisseur de données, comme le nombre maximal de fichiers journaux du fournisseur de données, la taille maximale du fichier journal et le niveau de détail inclus.

Le tableau ci-après contient une description détaillée des paramètres du fournisseur de données.

Tableau 181. Noms et descriptions des paramètres de configuration du fournisseur de données

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	Nom de l'instance. **Restriction :** La zone **Nom d'instance** affiche le nom de l'instance que vous indiquez la première fois que vous configurez l'agent. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.	Oui

Tableau 181. Noms et descriptions des paramètres de configuration du fournisseur de données (suite)

Nom du paramètre	Description	Zone obligatoire
Certificats SSL valides	Indique si l'agent valide des certificats SSL lorsqu'il utilise SSL pour communiquer sur le réseau. Définissez la valeur `Yes` si vous souhaitez que l'agent valide des certificats SSL lorsqu'il utilise SSL pour communiquer sur le réseau. Indiquez la valeur `No` pour empêcher l'agent de valider les certificats SSL. La valeur par défaut est `Oui`. Pour plus d'informations sur l'ajout d'un certificat SSL de source de données dans le magasin de certificats de confiance de l'agent, voir «Activation de la communication SSL avec les sources de données VMware VI», à la page 743.	Oui
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log	Taille maximale en ko qu'un fichier journal du fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Level of Detail in Data Provider Log	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est INFO. Les valeurs admises sont les suivantes : OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST et ALL.	Oui

Augmentation de la taille de segment de mémoire Java

Après avoir configuré l'Agent VMware VI, si vous surveillez un environnement d'infrastructure virtuelle VMware de grande taille, vous devrez sans doute augmenter la taille de segment de mémoire pour le fournisseur de données de Java™.

Pourquoi et quand exécuter cette tâche

La taille de segment de mémoire maximale par défaut du fournisseur de données Java est de 256 mégaoctets. Vous devez définir la taille de segment de mémoire maximale sur une valeur appropriée qui dépend de la taille de l'environnement VMware. Pour plus d'informations sur les tailles de segment de mémoire requises pour les différents environnements VMware, voir tableau 179, à la page 743.

Important : Le système sur lequel vous installez et configurez l'Agent VMware VI doit disposer d'un espace mémoire suffisant pour pouvoir s'adapter à la taille de segment de mémoire requise.

Si l'un des problèmes suivants survient, il peut s'avérer nécessaire d'augmenter la taille de segment de mémoire :

- Le fournisseur de données Java s'arrête en raison d'un problème `javacore` et crée un fichier nommé `javacore.`*`date.heure.numéro`*`.txt` dans le répertoire `CANDLEHOME\tmaitm6_x64`.
- Le fichier `javacore.`*`date.heure.numéro`*`.txt` contient la chaîne `java/lang/OutOfMemoryError`.

Procédure

- Windows Pour définir une taille de segment de mémoire de 1 Go, procédez comme suit :
  1. Ouvrez le fichier `%CANDLE_HOME%\TMAITM6_x64\kvm_data_provider.bat`.
  2. Ajoutez la ligne suivante avant la ligne qui commence par `KVM_JVM_ARGS="%KVM_CUSTOM_JVM_ARGS...` :

     ```
     SET KVM_CUSTOM_JVM_ARGS=-Xmx1024m
     ```
  3. Redémarrez l'agent.

- Linux Pour définir une taille de segment de mémoire de 1 Go, procédez comme suit :
  1. Ouvrez le fichier `$CANDLEHOME/lx8266/vm/bin/kvm_data_provider.sh`.
  2. Ajoutez la ligne suivante avant la ligne commençant par `KVM_JVM_ARGS="$KVM_CUSTOM_JVM_ARGS...` :
     `KVM_CUSTOM_JVM_ARGS=-Xmx1024m`
  3. Redémarrez l'agent.

Configuration de la surveillance de WebLogic

L'Monitoring Agent for WebLogic permet de surveiller de manière centralisée la santé, la disponibilité et les performances de votre environnement de serveur WebLogic. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant vos ressources WebLogic, y compris les machines virtuelles Java, le service de messagerie Java et la connectivité Java Database Connectivity (JDBC).

Avant de commencer

- Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 182.

Tableau 182. Versions d'agent

Version d'agent	Documentation
8.1.4, 8.1.4.1	Cloud APM 8.1.4 [2]
8.1.3.2	IBM Performance Management 8.1.3 [1]

[1] Le lien ouvre une rubrique Knowledge Center sur site.

[2] Le suivi des transactions et le diagnostic approfondi sont activés sur l'édition d'avril 2018 de l'agent version 8.1.4.1 sous AIX. Les versions précédentes de l'agent ne prenaient en charge que le suivi des transactions et le diagnostic approfondi sous Linux et Windows.

- Assurez-vous que votre environnement possède la configuration système requise pour l'Agent WebLogic. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent WebLogic.
- Avant de configurer l'Agent WebLogic, le serveur Oracle WebLogic doit d'abord être configuré en procédant comme suit :

  Remarque : La majorité de la configuration du serveur Oracle WebLogic est effectuée via la console d'administration, habituellement sur `http://weblogic-server:7001/console`.

  1. Configurez l'utilisateur du moniteur dans le groupe Monitors.
     a. Sélectionnez le domaine à surveiller ou modifier.
     b. Sélectionnez **Domaines de sécurité**.
     c. Sélectionnez votre domaine de sécurité (ou créez-en un s'il n'y en a aucun).
     d. Créez un utilisateur qui sera utilisé pour communiquer avec WebLogic via JMX.
     e. Ajoutez cet utilisateur au groupe Monitors.
     f. Sauvegardez les modifications apportées au domaine.
  2. Activez les ports d'écoute.
     a. Sélectionnez le domaine à surveiller ou modifier.
     b. Sur chaque serveur que vous souhaitez surveiller, cliquez sur **Environnement** > **Serveurs** > ***Sélectionner un serveur***.
     c. Vérifiez que le **port d'écoute** est activé et notez son numéro.
     d. Si vous souhaitez activer SSL, assurez-vous que le **port d'écoute SSL** est activé puis définissez aussi un port pour SSL.

3. Activez les connexions au serveur JMX MBean.
   a. Sélectionnez le domaine que vous souhaitez surveiller ou modifier.
   b. Sélectionnez **Configurer** > **Avancé**.
   c. Vérifiez l'option **Platform Mbean Server Enabled**.
   d. Sauvegardez la modification.
4. Activez l'option Protocole IIOP.
   a. Sélectionnez le domaine que vous souhaitez surveiller ou modifier.
   b. Sur chaque serveur que vous souhaitez surveiller, cliquez sur **Environnement** > **Serveurs**, puis sélectionnez un serveur.
   c. Sélectionnez l'**onglet Protocole** > ***Sélectionner IIOP***.
   d. Dans la section **Avancé**, saisissez le nom d'utilisateur et le mot de passe IIOP par défaut.
   e. Sauvegardez la modification.
5. Activez SSL.
   a. Activez HTTP Tunneling.
      1) Allez sur **Environnement** > **Serveurs** > ***Sélectionner un serveur*** > **Protocole** > **Général**.
      2) Vérifiez l'option **Activer HTTP Tunneling**.
   b. Activez le port d'écoute SSL.
      1) Allez sur **Environnement** > **Serveurs** > ***Sélectionner un serveur*** > **Configuration** > **Général**.
      2) Configurez un numéro de port.

Pourquoi et quand exécuter cette tâche

L'Agent WebLogic est un agent à plusieurs instances et à plusieurs sous-noeuds. Vous pouvez créer une instance d'agent à plusieurs sous-noeuds - un pour chaque serveur WebLogic ou une instance d'agent pour chaque serveur WebLogic avec un sous-noeud pour ce serveur. Vous pouvez également créer une combinaison de chaque type de configuration. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement.

Procédure

1. Pour configurer l'agent sur les systèmes Windows, utilisez la fenêtre IBM Performance Management ou le fichier de réponses silencieux avec le fichier de commandes de configuration.
   - «Configuration de l'agent sur des systèmes Windows», à la page 752.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 756.
2. Pour configurer l'agent sur les systèmes Linux et UNIX, exécutez le script de configuration de l'agent et répondez aux invites ou utilisez le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 755.
   - «Configuration de l'agent en utilisant le fichier de réponses silencieux», à la page 756.
3. Facultatif : Pour configurer le suivi des transactions, configurez les instances d'agent individuelles pour fournir les données de suivi des transactions et configurez votre Tableau de bord d'Application Performance pour afficher les données de suivi des transactions.
   a. Suivez la procédure pour «Configuration du suivi des transactions pour l'Agent WebLogic», à la page 758.
   b. Suivez la procédure pour «Configuration de votre Tableau de bord d'Application Performance pour l'affichage des données de suivi des transactions de l'Agent WebLogic», à la page 765.

   Remarque : La fonction de suivi des transactions est disponible pour l'Agent WebLogic dans l'offre Cloud APM, Advanced. Pour l'Agent WebLogic avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez cette étape.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent WebLogic sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Performance Management, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for WebLogic**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple : `weblogic01`.

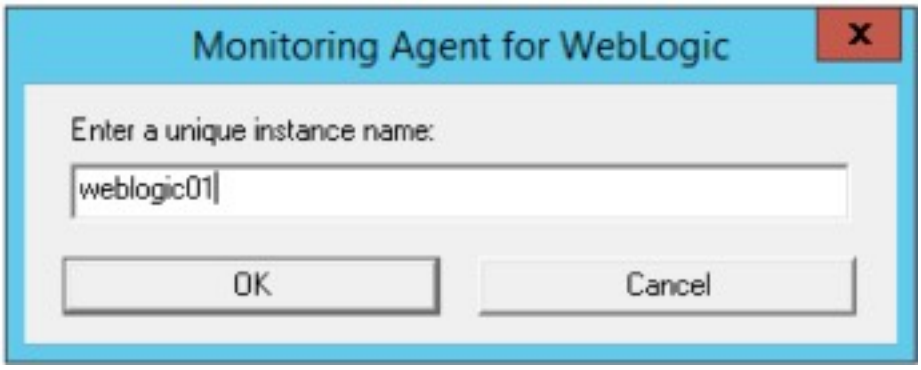


Figure 27. Fenêtre de saisie d'un nom d'instance unique

4. Cliquez sur **Suivant** dans le panneau de configuration de l'agent **Nom d'instance**.

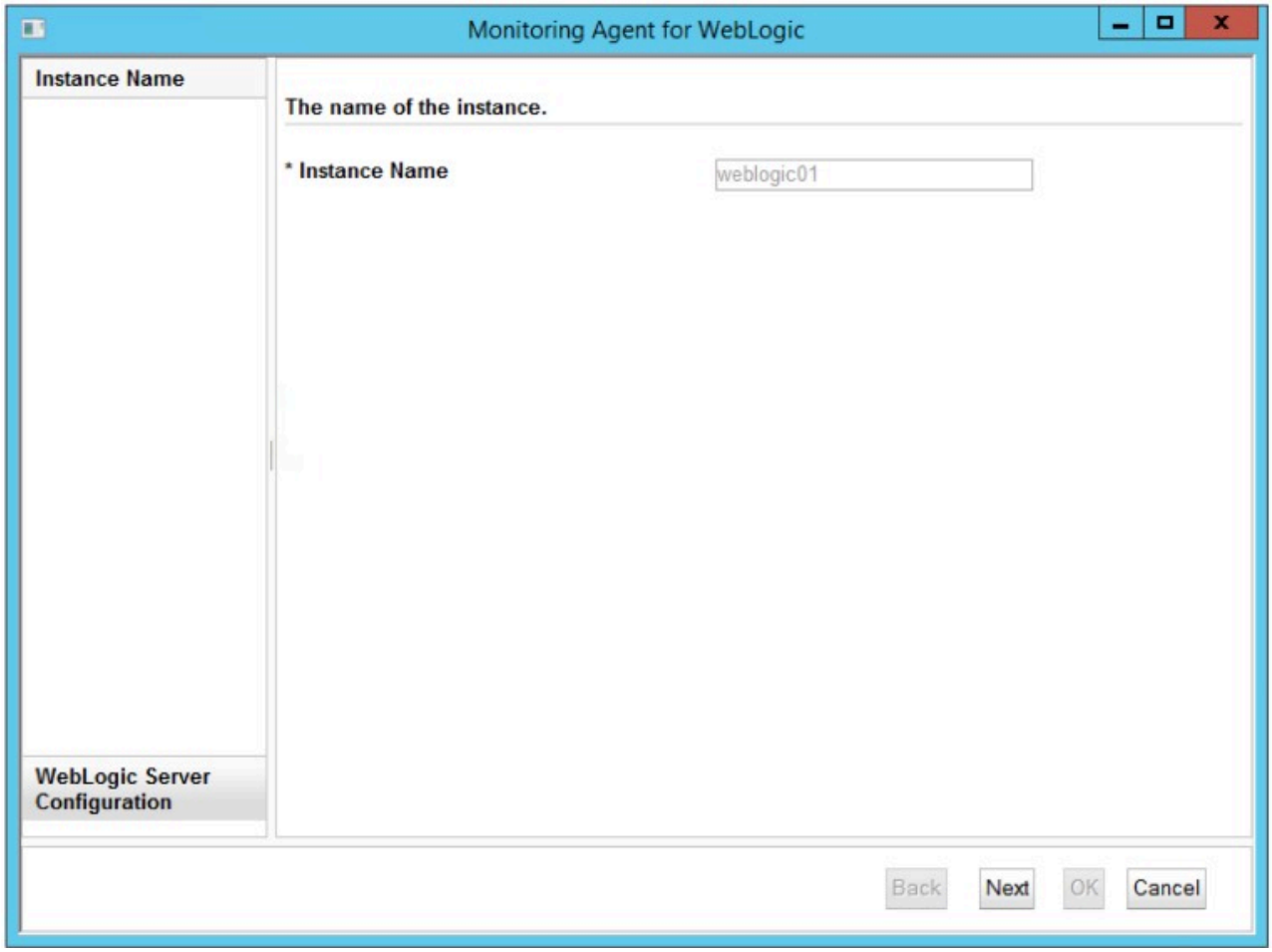


Figure 28. Fenêtre d'affichage du nom d'instance de l'agent

5. Entrez les paramètres du modèle d'instance de **Configuration du serveur WebLogic**.

   Remarque : Cette section ne décrit pas la configuration de l'instance de connexion au serveur WebLogic. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut lorsque vous ajoutez les configurations d'instance de connexion au serveur WebLogic réelles à partir de l'étape 6. Pour obtenir une description de chaque paramètre de configuration, voir tableau 183, à la page 758.

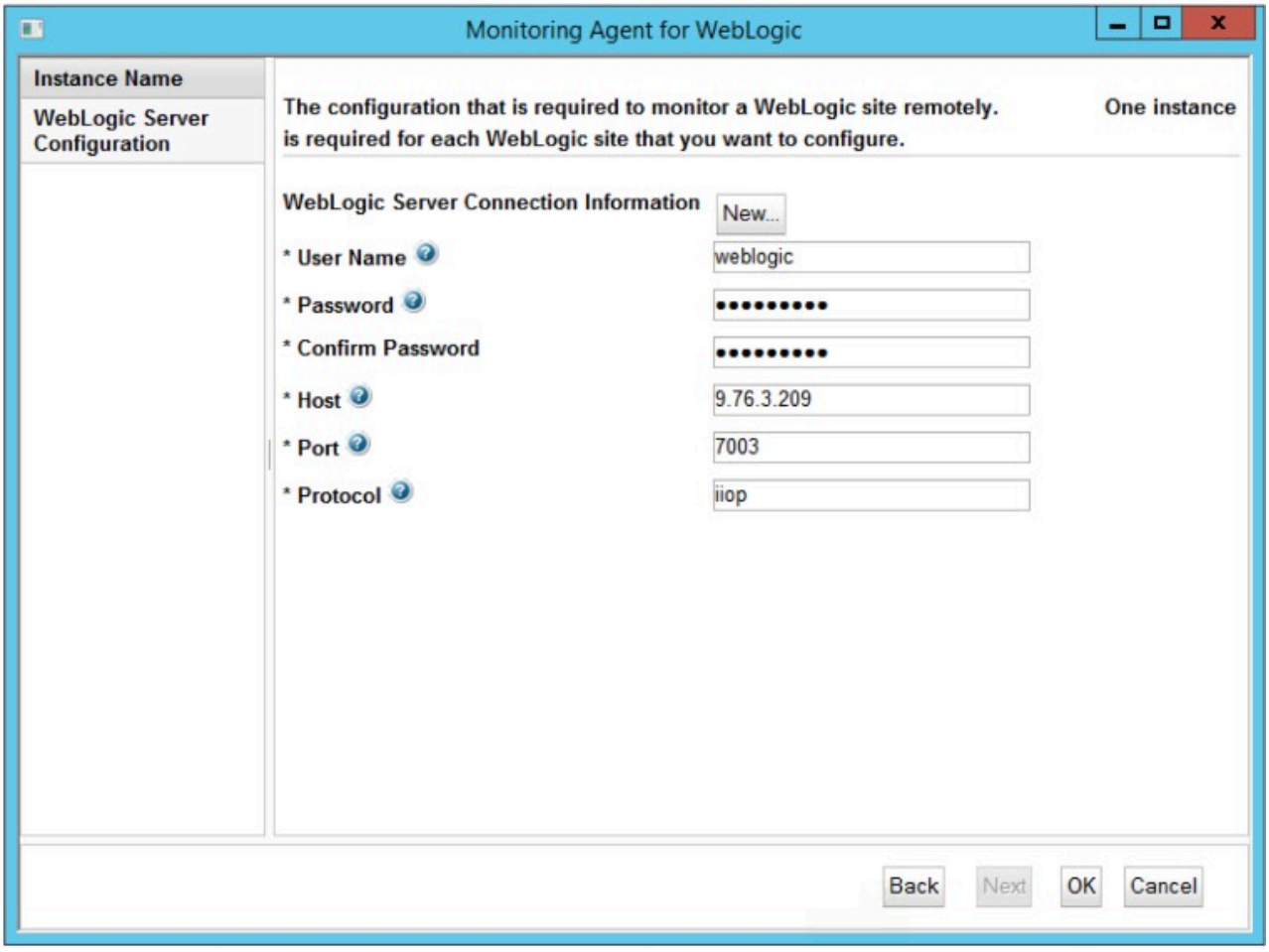


Figure 29. Fenêtre de spécification des paramètres du modèle d'instance de connexion au serveur WebLogic

6. Cliquez sur **Nouveau** et entrez les paramètres d'instance de connexion au serveur WebLogic, puis cliquez sur **Suivant**. Pour obtenir une description de chaque paramètre de configuration, voir tableau 183, à la page 758.

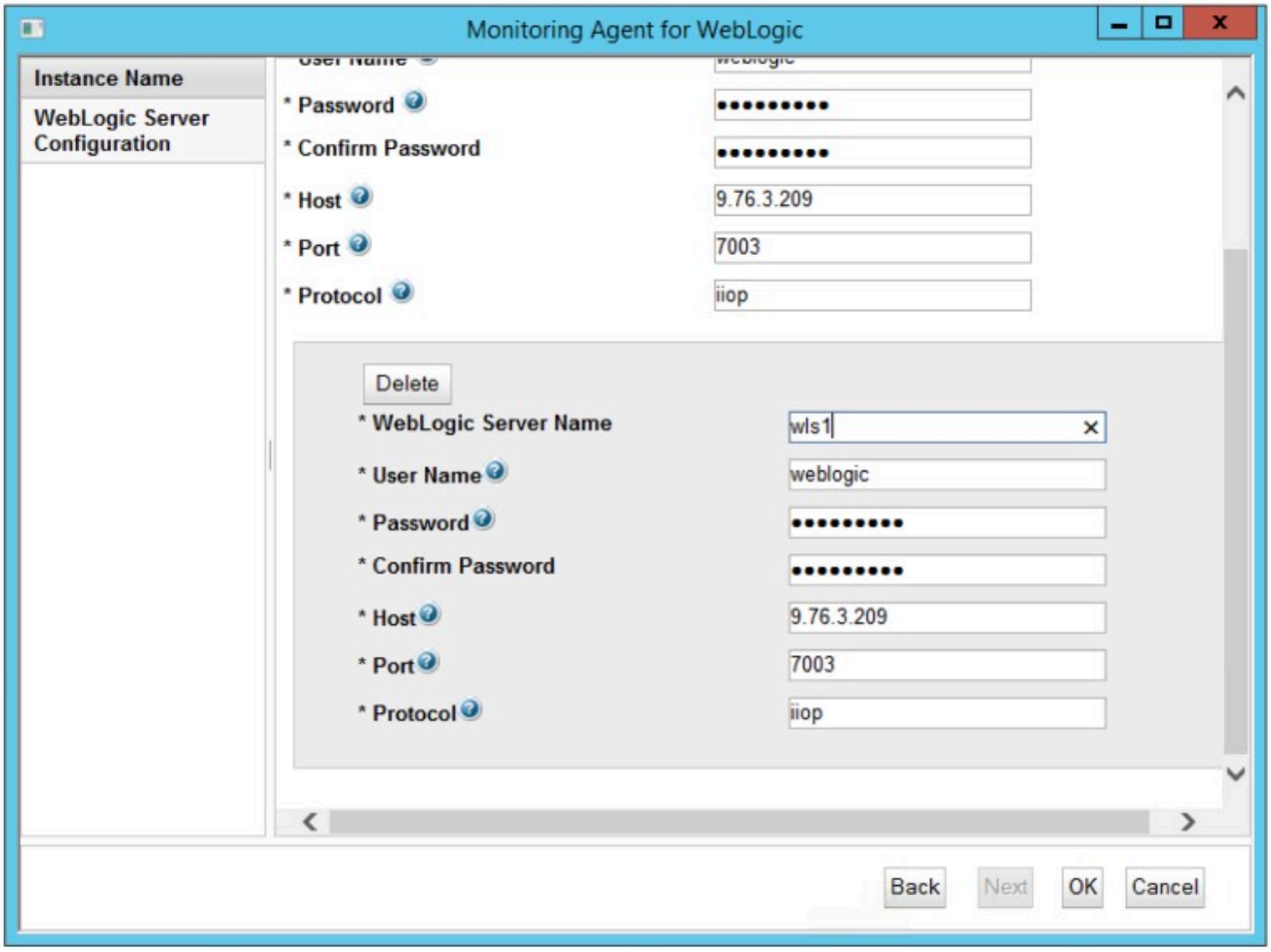


Figure 30. Fenêtre de spécification des paramètres d'instance de connexion au serveur WebLogic

7. Cliquez sur **OK** pour terminer la configuration.
8. Copiez les fichiers de sécurité de WebLogic dans le répertoire des fichiers binaires de l'Agent WebLogic.
   a. Localisez les fichiers `wlclient.jar` et `wljmxclient.jar` dans `ORACLE_HOME`. Par exemple, `C:\Oracle\Middleware\Oracle_Home\wlserver\server\lib`.
   b. Copiez les fichiers de l'étape 8a dans le répertoire des fichiers binaires de l'Agent WebLogic.
      - Linux AIX *rép_install*`/bin`.
      - Windows *rép_install*`\TMAITM6_x64`

      où *rép_install* représente le chemin d'installation de l'agent. Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
      - Linux AIX `/opt/ibm/apm/agent`
      - Windows `C:\IBM\APM\TMAITM6_x64`
9. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'Agent WebLogic, vous devez le configurer pour pouvoir le démarrer. Si l'Agent WebLogic est installé sur un ordinateur Linux ou UNIX local, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'Agent WebLogic en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   rép_install/bin/weblogic-agent.sh config **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent WebLogic», à la page 758.

3. Copiez les fichiers de la bibliothèque client WebLogic dans le répertoire des fichiers binaires de l'Agent WebLogic.

   a. Localisez les fichiers `wlclient.jar` et `wljmxclient.jar` dans `ORACLE_HOME`.

   b. Copiez les fichiers de l'étape 3a dans le répertoire des fichiers binaires de l'Agent WebLogic.

      rép_install/bin

   où *rép_install* représente le chemin d'installation de l'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin
   ```

4. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/weblogic-agent.sh start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent. Exemple

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01
   ```

Configuration de l'agent en utilisant le fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Configurez l'Agent WebLogic en mode silencieux en effectuant les étapes ci-après.

1. Dans un éditeur de texte, ouvrez le fichier `weblogic_silent_config.txt` disponible à l'emplacement suivant :

- Linux AIX *rép_install*/samples/weblogic_silent_config.txt
- Windows *rép_install*\samples\weblogic_silent_config.txt

où *rép_install* représente le chemin d'installation de l'agent. Exemple

- Linux AIX /opt/ibm/apm/agent/samples/weblogic_silent_config.txt
- Windows C:\IBM\APM\samples\weblogic_silent_config.txt

2. Dans le fichier weblogic_silent_config.txt, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent WebLogic», à la page 758.

3. Enregistrez et fermez le fichier weblogic_silent_config.txt et exécutez la commande suivante :

   - Linux AIX *rép_install*/bin/weblogic-agent.sh config **nom_instance** *rép_install*/samples/weblogic_silent_config.txt
   - Windows *rép_install*\bin\weblogic-agent.bat config **nom_instance** *rép_install*\samples\weblogic_silent_config.txt

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :

   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
   Exemple

   - Linux AIX /opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/weblogic_silent_config.txt
   - Windows C:\IBM\APM\bin\weblogic-agent.bat config example-inst01 C:\IBM\APM\samples\weblogic_silent_config.txt

4. Copiez les bibliothèques client de WebLogic dans le répertoire des fichiers binaires de l'Agent WebLogic.

   a. Localisez les fichiers wlclient.jar et wljmxclient.jar dans ORACLE_HOME.

   b. Copiez les fichiers de l'étape 4a dans le répertoire des fichiers binaires de l'Agent WebLogic.

      - Linux AIX *rép_install*/bin.
      - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent. Les chemins d'accès *rép_install* par défaut sont répertoriés ici :

   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

5. Exécutez la commande suivante pour démarrer l'agent :

   - Linux AIX *rép_install*/bin/weblogic-agent.sh start **nom_instance**
   - Windows *rép_install*\bin\weblogic-agent.bat start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :

   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   Exemple

- Linux AIX `/opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01`
- Windows `C:\IBM\APM\bin\weblogic-agent.bat start example-inst01`

Paramètres de configuration de l'Agent WebLogic

Les paramètres de configuration de l'Agent WebLogic sont regroupés dans un tableau.

1. Paramètres de l'agent WebLogic - Paramètres de l'environnement de l'agent WebLogic.

Tableau 183. Paramètres de l'agent WebLogic

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du serveur WebLogic	Indiquez un nom pour identifier l'instance de l'agent du serveur WebLogic. Exemple : *wls1* **Remarque :** Cet alias vous permet de représenter l'instance de l'agent du serveur WebLogic avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.	Chacun des paramètres suivants doit avoir un suffixe de nom d'instance qui sera le même pour chaque paramètre d'une instance d'agent. Les nouvelles instances d'agent doivent utiliser un nom d'instance unique pour son jeu de paramètres. Par exemple, une instance d'agent peut utiliser *.wls1* et une autre instance d'agent peut utiliser *.wls*2 à la place de *.nom_instance* dans les noms de paramètres ci-dessous.
Nom d'utilisateur	Nom d'utilisateur utilisé pour s'authentifier avec le serveur WebLogic.	**KWB_WLS_USERNAME.nom_instance**
Mot de passe	Mot de passe utilisé pour s'authentifier avec le serveur WebLogic.	**KWB_WLS_PASSWORD.nom_instance**
Hôte	Hôte utilisé pour s'authentifier avec le serveur WebLogic. Entrez le nom d'hôte qualifié complet ou l'adresse IP du serveur WebLogic.	**KWB_WLS_HOST.nom_instance**
Port	Port utilisé pour s'authentifier avec le serveur WebLogic.	**KWB_WLS_PORT.nom_instance**
Protocole	Protocole utilisé pour s'authentifier avec le serveur WebLogic. Les protocoles pris en charge sont *iiop* et *https*.	**KWB_WLS_PROTOCOL.nom_instance**

Configuration du suivi des transactions pour l'Agent WebLogic

La fonction de suivi des transactions de l'Agent WebLogic requiert des modifications dans le fichier des paramètres d'environnement de l'instance d'agent et le fichier de démarrage du serveur WebLogic. Un script est fourni pour vous aider à apporter ces modifications.

Avant de commencer

Linux AIX Vérifiez que la limite de ressource pour les fichiers ouverts est supérieure à 5 000 pour que le kit d'outils de suivi des transactions fonctionne correctement.

- Affichez le paramètre de limite de fichiers ouverts en cours. **ulimit -n**
- Exemple de paramètre définissant la limite de fichiers ouverts à 5 056. **ulimit -n 5056**

Exécutez l'Windows étape 1 ou l'Linux AIX étape 2 de «Configuration de la surveillance de WebLogic», à la page 750 avant de suivre cette procédure.

Remarque : La fonction de suivi des transactions est disponible pour l'Agent WebLogic dans l'offre Cloud APM, Advanced. Pour l'Agent WebLogic avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez cette étape.

L'Agent WebLogic doit être installé en local sur le serveur WebLogic surveillé avec la fonction de suivi des transactions.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *WEBLOGIC_HOME*.
2. Répertoire *WEBLOGIC_HOME*/bin et ses fichiers.
3. Répertoire *rép_install*/config.
4. Fichier *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg.

où

WEBLOGIC_HOME
Répertoire d'installation du serveur WebLogic.

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 752
- Configuration de l'agent en répondant à des invites, étape 1, à la page 756
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 2, à la page 757

Procédure

Exécutez le script **simpleConfig**.

1. Connectez-vous au serveur WebLogic sur lequel l'Agent WebLogic est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux AIX *rép_install*
   - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
3. Accédez au répertoire wbdchome/8.1.4.0.0/bin.
4. Exécutez le script d'installation.
   - Linux AIX ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Suivez les invites pour entrer des paramètres pour votre environnement :
   a. Choisissez l'Agent WebLogic *nom_instance* et le sous-noeud à configurer dans la liste des combinaisons d'instance d'agent et de sous-noeud détectées, *nom_instance* représentant le nom de l'instance d'agent.
   b. Indiquez le numéro de la méthode de démarrage du serveur WebLogic.

c. Indiquez le chemin de recherche racine du domaine WebLogic. Ce chemin d'accès est utilisé comme base pour la recherche de domaines WebLogic. Si la variable d'environnement *WEBLOGIC_HOME* est définie, sa valeur est offerte en tant que valeur par défaut.

d. Indiquez le numéro du domaine WebLogic pour le serveur WebLogic à configurer.

e. Entrez le numéro du nom de serveur WebLogic à configurer.

Linux Exemple de configuration avec une méthode de démarrage WebLogic `Script de démarrage WebLogic`.

```
./simpleconfig.sh

Les agents et sous-noeuds suivants ne sont pas encore configurés pour le suivi des transactions :

1) wlinst1 Server1
2) wlinst1 Server2

Entrez le numéro qui correspond à l'instance d'agent et au sous-noeud que vous voulez configurer.

Indiquez votre sélection ici (par exemple : 1) : 1

Les méthodes de démarrage WebLogic suivantes sont prises en charge :

1) Script de démarrage WebLogic
2) Gestionnaire de noeud WebLogic

Indiquez votre sélection ici (par défaut 1) : 1

Chemin d'accès pour commencer la recherche des domaines WebLogic.
Chemin de recherche du domaine WebLogic (par défaut) : /home/wlsadmin

Voici les chemins d'accès au domaine WebLogic trouvés :

1) /home/wlsadmin/oracle/user_projects/domains/ttdd

Entrez le numéro qui correspond au domaine WebLogic contenant le serveur WebLogic que
vous souhaitez configurer.

Entrez votre sélection ici (par exemple : 1) : 1

Les serveurs WebLogic suivants sont disponibles pour configuration :

1) AdminServer
2) Server1

Sélectionnez un nom de serveur WebLogic (par défaut : 2) : 2
INFO: [2000] Automatic configuration of agent environment file succeeded.
INFO: [3000] Automatic configuration of WebLogic start script succeeded.
INFO: [9000] Restart the WebLogic agent and WebLogic server for configuration to take effect.
```

6. Suivez ces étapes si `Gestionnaire de noeud WebLogic` est sélectionné comme **Méthode de démarrage du serveur WebLogic** à l'étape 5b, à la page 759. Sinon, passez à l'étape 7, à la page 762.

   a. Ouvrez le fichier `weblogic_nodemanager_dc_opts` répertorié dans le message d'information numéro 3011 du texte de sortie à l'étape 5, à la page 759.

   Windows Exemple de sortie de configuration avec la méthode de démarrage WebLogic `Gestionnaire de noeud WebLogic`.

   ```
   INFO: [2000] Automatic configuration of agent environment file succeeded.
   INFO: [3010] Automatic configuration of WebLogic start script skipped.
   INFO: [3011] Please review C:\IBM\APM\TMAITM6_x64\wbdchome\8.1.4.0.0\runtime\ttdd_win\win_Server1\
   staging\weblogic_nodemanager_dc_opts.win for required WebLogic JVM start options.
   INFO: [9000] Restart the WebLogic agent and WebLogic server for configuration to take effect.
   ```

   b. Connectez-vous à la console WebLogic et sélectionnez **Environnement** > **Serveurs**.

   c. Sélectionnez le serveur à configurer.

   d. Sélectionnez l'onglet **Configuration** > **Server Start**.

e. Copiez les arguments de démarrage du serveur à partir du fichier `weblogic_nodemanager_dc_opts` vers les arguments **Start Server** du serveur dans la console WebLogic et sauvegardez les modifications. Les arguments de démarrage du serveur correspondent à toutes les lignes qui suivent la ligne de commentaire `# Add the following lines to the server start arguments` dans le fichier `weblogic_nodemanager_dc_opts`.

f. Vérifiez que le kit d'outils de suivi des transactions se trouve dans le chemin de la bibliothèque partagée lors de l'exécution. Choisissez une méthode.

- Mettez à jour le script de démarrage du gestionnaire de noeud.

  Remarque : Tous les serveurs WebLogic démarrés par le gestionnaire de noeud ont ce chemin d'accès à la bibliothèque défini avec les bibliothèques de fichiers objets du kit d'outils de suivi des transactions incluses.

  1) Ouvrez le fichier `weblogic_nodemanager_dc_opts` répertorié dans le message d'information numéro 3011 du texte de sortie à l'étape 5, à la page 759.
  2) Définissez le chemin du kit d'outils de suivi des transactions dans le script de démarrage du gestionnaire de noeud. La commande permettant de définir le chemin est la ligne qui suit la ligne de commentaire `# Make sure that the executable path available to the WebLogic server includes the toolkit lib directory` dans le fichier `weblogic_nodemanager_dc_opts`.
     - Linux Copiez la ligne LD_LIBRARY_PATH line à partir du fichier `weblogic_nodemanager_dc_opts.linux` généré et copiez-la sous la ligne `export JAVA_OPTIONS` dans le script de démarrage du gestionnaire de noeud. Exemple : *WEBLOGIC_HOME*`/user_projects/domains/`*nom_domaine*`/bin/startNodeManager.sh`.
     - Windows Copiez la ligne PATH à partir du fichier `weblogic_nodemanager_dc_opts.win` généré et copiez-la sous la ligne `export JAVA_OPTIONS` dans le script de démarrage du gestionnaire de noeud. Exemple : *WEBLOGIC_HOME*`\user_projects\domains\`*nom_domaine*`\bin\startNodeManager.bat`.

     où *WEBLOGIC_HOME* représente le répertoire d'installation du serveur WebLogic et *nom_domaine*, le nom du domaine WebLogic.

- Mettez à jour l'environnement pour le compte utilisateur qui démarre le gestionnaire de noeud.

  Remarque : Toutes les applications démarrées par le compte utilisateur ont ce chemin d'accès à la bibliothèque défini avec les bibliothèques de fichiers objets du toolkit incluses.

  1) Modifiez les paramètres d'environnement pour l'utilisateur qui démarre le gestionnaire de noeud.
     - Linux AIX Modifiez le fichier de ressources de shell ou le fichier de profils de shell. Par exemple : `.bashrc` ou `.bash_profile`.
     - Windows Modifiez **Panneau de configuration** > **Système et sécurité** > **Système** > **Paramètres système avancés** > **Variables d'environnement** > **Variables utilisateur pour *nom_utilisateur*** > **Chemin**, *nom_utilisateur* représentant le nom du compte utilisateur utilisé pour démarrer le serveur WebLogic.
  2) Définissez le chemin du kit d'outils de suivi des transactions dans l'environnement du compte utilisateur. La commande permettant de définir le chemin est la ligne qui suit la ligne de commentaire `# Make sure that the executable path available to the WebLogic server includes the toolkit lib directory` dans le fichier `weblogic_nodemanager_dc_opts`.
     - Linux AIX Copiez la ligne `export LD_LIBRARY_PATH` à partir du fichier `weblogic_nodemanager_dc_opts.linux` généré. Si une ligne `export LD_LIBRARY_PATH` n'existe pas, ajoutez-la. Si elle existe, modifiez-la pour ajouter uniquement le chemin situé à droite du signe égal dans le chemin existant avec le délimiteur de chemin correct.
     - Windows Copiez la ligne `set PATH` à partir du fichier `weblogic_nodemanager_dc_opts.win` généré. Si une variable **Path** n'existe pas dans la section **User variables for *nom_utilisateur*** (*nom_utilisateur* représentant le nom du compte utilisateur utilisé pour démarrer le serveur WebLogic), ajoutez-la en entrant `Path` comme nom de variable et le

chemin situé à droite du signe égal comme valeur. Si elle existe, modifiez la valeur pour ajouter uniquement le chemin situé à droite du signe égal dans le chemin existant avec le délimiteur de chemin correct.

3) Rechargez l'environnement.

Remarque : Les scripts `startNodeManager` sont générés par l'utilitaire de configuration WebLogic. Vous risquez de perdre vos modifications lorsque la configuration WebLogic sera exécutée à nouveau.

7. Si le serveur WebLogic et l'agent sont en cours d'exécution, redémarrez-les.

Résultats

Fichiers du serveur WebLogic modifiés lors de la configuration du suivi des transactions :

- Script `startManagedWebLogic`.
  - Linux AIX *WEBLOGIC_HOME*`/bin/startManagedWebLogic.sh`
  - Windows *WEBLOGIC_HOME*`\bin\startManagedWebLogic.cmd`

  où *WEBLOGIC_HOME* représente le répertoire d'installation du serveur WebLogic.

  Ce fichier est mis à jour avec les paramètres de configuration pour la fonction de suivi des transactions. Des repères de configuration sont insérés dans le fichier pour pouvoir être utilisés lorsque vous désactivez la fonction de suivi des transactions. Un fichier de sauvegarde est sauvegardé dans le répertoire *WEBLOGIC_HOME*`/bin/bak/` avant que le script ajoute ou supprime les modifications des fonctions de suivi des transactions.

Fichiers de l'agent modifiés lors de la configuration du suivi des transactions :

- Fichier de configuration de l'instance d'agent
  - Linux AIX *rép_install*`/config/`*nom_hôte*`_wb_`*nom_instance*`.cfg`
  - Windows *rép_install*`\TMAITM6_x64\`*nom_hôte*`_WB_`*nom_instance*`.cfg`
- Fichier des paramètres d'environnement de l'agent
  - Linux AIX *rép_install*`/config/wb_`*nom_instance*`.environment`
  - Windows *rép_install*`\TMAITM6_x64\KWBENV_`*nom_instance*

où

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 752
- Configuration de l'agent en répondant à des invites, étape 1, à la page 756
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 2, à la page 757

Désactivation du suivi des transactions pour une instance Agent WebLogic

La fonction de suivi des transactions de l'Agent WebLogic peut être supprimée. Un script est fourni pour supprimer la fonction de suivi des transactions pour une instance d'agent.

Avant de commencer

Assurez-vous que le serveur WebLogic et l'Agent WebLogic sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *WEBLOGIC_HOME*.
2. Répertoire *WEBLOGIC_HOME*/bin et ses fichiers.
3. Répertoire *rép_install*/config.
4. Fichier *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg.

Procédure

Exécutez le script **unconfig** avec l'option **remove**.

1. Connectez-vous au serveur WebLogic sur lequel l'Agent WebLogic est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux AIX *rép_install*
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire wbdchome/8.1.4.0.0/bin.
4. Exécutez **unconfig** avec l'option **remove**, le nom de l'instance d'agent et le nom du sous-noeud.
   - Pour désactiver un sous-noeud d'une instance d'agent, utilisez le paramètre *nom_sous_noeud*.
     - Linux AIX ./unconfig.sh **remove** *nom_instance nom_sous_noeud*
     - Windows unconfig.bat **remove** *nom_instance nom_sous_noeud*
   - Pour désactiver tous les sous-noeuds pour une instance d'agent, omettez le paramètre *nom_sous_noeud*.
     - Linux AIX ./unconfig.sh **remove** *nom_instance*
     - Windows unconfig.bat **remove** *nom_instance*
5. Démarrez l'agent et le serveur WebLogic.

où

WEBLOGIC_HOME
Répertoire d'installation du serveur WebLogic.

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 752
- Configuration de l'agent en répondant à des invites, étape 1, à la page 756
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 2, à la page 757

nom_sous_noeud
Nom du sous-noeud de l'instance d'agent affecté au paramètre **Nom du serveur WebLogic** dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 6, à la page 754
- Configuration de l'agent en répondant à des invites, étape 2, à la page 756
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 2, à la page 757

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

Désinstallation du suivi des transactions pour l'Agent WebLogic

La fonction de suivi des transactions de l'Agent WebLogic peut être désinstallée. Un script est fourni pour supprimer la fonction de suivi des transactions de toutes les instances d'agent, ainsi que le kit d'outils de suivi des transactions.

Avant de commencer

Assurez-vous que le serveur WebLogic et toutes les instances d'Agent WebLogic sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *WEBLOGIC_HOME*.
2. Répertoire *WEBLOGIC_HOME*/bin et ses fichiers.
3. Répertoire *rép_install*/config.
4. Fichier *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg.

Procédure

Exécutez le script **unconfig** avec l'option **uninstall**.

1. Connectez-vous au serveur WebLogic sur lequel l'Agent WebLogic est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux AIX *rép_install*
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire wbdchome/8.1.4.0.0/bin.
4. Exécutez **unconfig** avec l'option **uninstall**.
   - Linux AIX `./unconfig.sh uninstall`
   - Windows `unconfig.bat uninstall`
5. Démarrez le serveur WebLogic et toutes les instances d'agent.

où

WEBLOGIC_HOME
Répertoire d'installation du serveur WebLogic.

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape 3, à la page 752
- Configuration de l'agent en répondant à des invites, étape 1, à la page 756
- Configuration de l'agent en utilisant le fichier de réponses silencieux, étape 2, à la page 757

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

Configuration de votre Tableau de bord d'Application Performance pour l'affichage des données de suivi des transactions de l'Agent WebLogic

Pour afficher les données rassemblées par la fonction de suivi des transactions de l'Agent WebLogic, des modifications doivent être apportées à la configuration de votre Tableau de bord d'Application Performance.

Avant de commencer

Effectuez l'étape «Configuration du suivi des transactions pour l'Agent WebLogic», à la page 758 avant de suivre cette procédure.

Procédure

1. Activez les données de suivi des transactions dans le Tableau de bord d'Application Performance si vous disposez de l'Agent WebLogic avec la fonction de suivi des transactions, qui est disponible dans l'offre Cloud APM, Advanced et que vous souhaitez activer la fonction de suivi des transactions.
   a. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
   b. Sélectionnez l'onglet **WebLogic**.
   c. Sélectionnez les cases à cocher pour les instances de l'agent du serveur WebLogic que vous souhaitez surveiller et effectuez l'une des actions suivantes figurant dans la liste **Actions** :
      - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking (Définir le suivi des transactions)** > **Activé**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Enabled*.
      - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Désactivé**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Disabled*.
2. Pour visualiser les tableaux de bord des données de suivi des transactions de l'Agent WebLogic, ajoutez l'instance de l'Agent WebLogic à une applications de votre Tableau de bord d'Application Performance. Pour plus d'informations sur l'éditeur d'applications, voir Gestion des applications.
3. Assurez-vous que des comptes utilisateur sont affectés à un rôle qui inclut les droits d'accès au Tableau de bord de diagnostic de façon à pouvoir accéder aux boutons suivants du Tableau de bord des applications pour le suivi des transactions de l'Agent WebLogic. Sinon, ces boutons sont désactivés pour ces utilisateurs dans le Tableau de bord des applications.
   a. Le bouton d'analyse détaillée **Diagnostiquer** sur le widget **Slowest 5 Response Time** (Temps de réponse - les 5 les plus lents).
   b. Le bouton **Inflight Requests** sur le widget **Applications**.

Configuration de la surveillance des applications WebSphere

La configuration de la surveillance des applications WebSphere implique la configuration d'un collecteur de données pour vos serveurs d'applications. Le collecteur de données peut être autonome ou imbriqué à l'Agent WebSphere Applications.

Collecteur de données imbriqué

La plupart des serveurs d'applications WebSphere peuvent être surveillés par le collecteur de données imbriqué, excepté pour le profil Liberty sur IBM Cloud. Le collecteur de données imbriqué peut fournir toutes les fonctions de surveillance disponibles.

Pour configurer le collecteur de données imbriqué, vous devez au préalable installer l'Agent WebSphere Applications sur le système sur lequel le serveur d'applications est en cours

d'exécution. Après cela, utilisez les utilitaires de configuration fournis pour configurer le collecteur de données de manière interactive ou silencieuse.

Collecteur de données autonome

Le collecteur de données autonome s'applique uniquement à WebSphere Application Server Liberty sous Linux for System x et au profil WebSphere Liberty sur IBM Cloud.

Si vous choisissez de configurer un collecteur de données autonome, vous pouvez ignorer la procédure d'installation de l'agent et configurer directement le collecteur de données dans Liberty.

Toutefois, certaines données de diagnostic à la demande, telles que le cliché de tas à l'heure actuelle ou les informations sur les demandes en cours, ne seront pas collectées par le collecteur de données autonome. Cela signifie que vous pouvez uniquement activer le collecteur de données de manière à ce qu'il collecte automatiquement les informations de cliché de tas à des intervalles spécifiés et que vous ne pouvez pas prendre d'instantané de segment de mémoire lorsque vous le souhaitez à l'aide du bouton **Take Snapshot** de la console Cloud APM. Les tableaux de bord associés aux demandes en cours qui peuvent être fournis par le collecteur de données imbriqué sont tous indisponibles au collecteur de données autonome.

Utilisez tableau 184 pour déterminer le collecteur de données approprié pour votre serveur d'applications.

Tableau 184. Applications WebSphere et collecteurs de données applicables

Application à surveiller	Collecteur de données applicable	Documentation
WebSphere Application Server Traditional	Collecteur de données imbriqué	«Configuration du collecteur de données pour l'Agent WebSphere Applications»
WebSphere Application Server Liberty (sur site)	• Collecteur de données imbriqué • Collecteur de données autonome (Linux for System x uniquement)	• «Configuration du collecteur de données pour l'Agent WebSphere Applications» • «Configuration du collecteur de données Liberty pour les applications sur site», à la page 813
Profil WebSphere Liberty sur IBM Cloud	Collecteur de données autonome	«Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 845
Profil WebSphere Liberty dans un conteneur Docker	Collecteur de données imbriqué	«Surveillance de WebSphere Application Server Liberty dans un conteneur Docker», à la page 800

Configuration du collecteur de données pour l'Agent WebSphere Applications

L'Agent WebSphere Applications n'a pas besoin d'être configuré après l'installation de l'agent, à moins que vous ne souhaitez modifier le port par défaut. Vous devez toutefois configurer le collecteur de données, qui est un composant de l'agent, pour configurer la surveillance pour votre environnement WebSphere.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 185.

Tableau 185. Versions d'agent

Version d'agent	Documentation
7.3.0.14.0, 7.3.0.14.01, 7.3.0.14.02, 7.3.0.14.03, 7.3.0.14.04, 7.3.0.14.05, 7.3.0.14.06	Cloud APM 8.1.4
7.3.0.11.0	IBM Performance Management 8.1.3

Tableau 185. Versions d'agent (suite)

Version d'agent	Documentation
7.3.0.10.0	IBM Performance Management 8.1.2
7.3.0.9.0	IBM Performance Management 8.1.1

Procédure

- (Version accélérée) Si vous n'utilisez que l'Agent WebSphere Applications sans l'ITCAM Agent for WebSphere Applications du produit hérité dans votre environnement, pour configurer rapidement l'environnement pour la surveillance, voir une procédure de configuration simplifiée dans la section «Version accélérée : configuration du collecteur de données pour l'Agent WebSphere Applications».
- (Configuration simple) Pour une procédure de configuration complète pour un environnement IBM Cloud Application Performance Management pur, voir la section «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 771.
- (Configuration complète) Pour configurer le collecteur de données avec plus d'options de personnalisation, utilisez les utilitaires de configuration complète. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.
- (Configuration en mode silencieux) Pour déployer la même surveillance pour plusieurs instances de serveur d'applications, configurez le collecteur de données en mode silencieux. Pour plus d'informations, voir «Configuration du collecteur de données en mode silencieux», à la page 782.
- (WebSphere Portal Server) Pour surveiller les instances WebSphere Portal Server, utilisez la procédure de configuration avancée. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.
- (Configuration manuelle) Si vous ne pouvez pas utiliser les utilitaires de configuration fournis pour configurer le collecteur de données pour l'Agent WebSphere Applications, configurez manuellement le collecteur de données dans la console d'administration WebSphere. Pour plus d'informations, voir «Configuration manuelle du collecteur de données si les utilitaires de configuration échouent», à la page 788.
- (Coexistence des agents) Pour configurer le collecteur de données de sorte qu'il fonctionne dans un environnement de coexistence des agents où l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications sont installés, voir «(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données», à la page 792.
- (Surveillance de Docker) Pour surveiller WebSphere Application Server Liberty s'exécutant dans un conteneur Docker, voir «Surveillance de WebSphere Application Server Liberty dans un conteneur Docker», à la page 800.

Version accélérée : configuration du collecteur de données pour l'Agent WebSphere Applications

L'Agent WebSphere Applications n'a pas besoin d'être configuré après l'installation de l'agent. Vous devez toutefois configurer le collecteur de données, qui est un composant de l'agent, pour configurer la surveillance pour votre environnement WebSphere.

Avant de commencer

1. Installez l'Agent WebSphere Applications sur le système où le serveur d'applications à surveiller est installé et en cours d'exécution.
2. Vérifiez les exigences d'accès utilisateur.
   - Windows Utilisez l'ID administrateur utilisé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose du droit complet en écriture sur le répertoire de base du collecteur de données, *rép_install*\dchome\7.3.0.14.06.

- Linux AIX Utilisez l'ID utilisateur employé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose de droits en lecture et en écriture sur les sous-répertoires suivants dans *rép_install*/yndchome/7.3.0.14.06 :
  - bin
  - data
  - runtime

Pourquoi et quand exécuter cette tâche

Un utilitaire de configuration simple, simpleconfig, est utilisé dans cette procédure pour fournir la configuration de base du collecteur de données.

L'utilitaire simpleconfig configure le collecteur de données avec les paramètres par défaut. Pour configurer le collecteur de données avec plus d'options de personnalisation, utilisez les utilitaires de configuration complète, config, dans le même répertoire. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.

Dans la plupart des cas, l'utilitaire simpleconfig suffit. Pour un environnement plus complexe, vous pouvez utiliser l'utilitaire de configuration config pour configurer le collecteur de données. Si l'utilitaire simpleconfig échoue, utilisez config à la place.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire bin au sein du répertoire de base du collecteur de données.
   - Windows *rép_install*\dchome\7.3.0.14.06\bin
   - Linux AIX *rép_install*/yndchome/7.3.0.14.06/bin
3. Exécutez l'utilitaire de configuration simple suivant:
   - Windows **simpleconfig.bat**
   - Linux AIX **./simpleconfig.sh**
4. Suivez les invites pour continuer la configuration du collecteur de données.

   Vous êtes tenu d'effectuer quelques-unes ou l'ensemble des actions suivantes selon les paramètres du serveur d'applications :
   - Pour un WebSphere Application Server traditionnel :
     - Sélectionnez le répertoire d'installation WebSphere découvert automatiquement ou indiquez-le manuellement.
     - Sélectionnez le profil WebSphere Application Server à surveiller.
     - Sélectionnez le profil des propriétés de sécurité à utiliser ou fournissez le nom d'utilisateur et le mot de passe de la console d'administration WebSphere (si la sécurité est activée pour le serveur d'applications).
   - Pour WebSphere Application Server Liberty :
     - Indiquez le chemin d'accès complet du répertoire de base Liberty qui contient les répertoires bin et servers. Par exemple, /opt/ibm/wlp.
     - Indiquez le répertoire de base du JRE qui est utilisé par Liberty.
5. Une fois que la configuration du collecteur de données est terminée, redémarrez le serveur d'applications.
   a. Accédez au répertoire bin situé sous le répertoire de base du profil de serveur d'applications. Par exemple, opt/IBM/WebSphere/AppServer/profiles/*nom_profil*/bin.
   b. Arrêtez le serveur d'applications en entrant la commande **stopServer** dans la console de commande.

- Linux AIX `./stopServer.sh nom_serveur`
- Windows `stopServer.bat nom_serveur`

c. A l'invite, entrez l'ID utilisateur et le mot de passe de l'administrateur de la console d'administration WebSphere.

d. Redémarrez le serveur d'applications en entrant la commande **startServer** dans la console de commande.

- Linux AIX `./startServer.sh nom_serveur`
- Windows `startServer.bat nom_serveur`

6. Connectez-vous à la console Cloud APM pour afficher les données dans les tableaux de bord.

a. Ouvrez une fenêtre de navigateur et entrez l'adresse URL suivante, où *hôte_serveur* correspond à l'adresse IP du serveur :

`https://hôte_serveur:9443`

b. Lorsque vous êtes invité à indiquer votre ID de connexion, entrez les données d'identification suivantes pour l'utilisateur par défaut ou entrez les données d'identification qui ont été affectées à votre administrateur de console Cloud APM :

- Nom d'utilisateur : *apmadmin*
- Mot de passe : *apmpass*

Les données d'identification utilisateur initiales après l'installation du serveur Cloud APM sont `apmadmin` avec le mot de passe `apmpass`.

c. Utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillé au Tableau de bord d'Application Performance. Vous pouvez l'ajouter en tant que nouveau composant à votre application existante ou créer une application à laquelle ajouter ce composant. Pour plus d'informations sur l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

Résultats

Le collecteur de données permet de surveiller l'instance de serveur d'applications. Gardez à l'esprit que la collecte de données peut augmenter la surcharge du serveur d'applications. Vous pouvez contrôler la collecte de données avec des options de configuration plus avancées pour l'optimisation.

Vérification des exigences d'accès utilisateur

L'Agent WebSphere Applications a certaines exigences d'accès utilisateur pour l'ID utilisateur qui doit configurer le collecteur de données.

Pourquoi et quand exécuter cette tâche

Utilisez l'ID employé pour installer le serveur d'applications pour configurer le collecteur de données après avoir accordé les droits appropriés à l'ID d'installation du serveur d'applications.

Procédure

- Windows Utilisez l'ID administrateur utilisé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose du droit complet en écriture sur le répertoire de base du collecteur de données, *rép_install*`\dchome\7.3.0.14.06`.
- Linux AIX Utilisez l'ID utilisateur employé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose de droits en lecture et en écriture sur les sous-répertoires suivants dans *rép_install*`/yndchome/7.3.0.14.06` :
  - `bin`
  - `data`
  - `logs`
  - `runtime`

A faire : Si vous utilisez des ID utilisateur différents pour installer les serveurs d'applications, vous devrez peut-être faire de même pour configurer le collecteur de données. Après avoir configuré le collecteur de données pour la première fois, accordez le droit en écriture sur les fichiers suivants chaque fois que vous utilisez un ID utilisateur différent pour configurer le collecteur de données, où *nom_profil* correspond au nom de profil du serveur d'applications :

- *rép_install*/yndchome/7.3.0.14.06/data/findservers.inputlist
- *rép_install*/yndchome/7.3.0.14.06/data/*profile_name*.findservers.progress
- *rép_install*/yndchome/7.3.0.14.06/data/config_inputlist
- *rép_install*/yndchome/7.3.0.14.06/runtime/custom/connections.properties

Gestion d'un autre collecteur de données existant dans le serveur d'applications

Si un collecteur de données existe déjà dans le serveur d'applications, vous devez décider quoi en faire afin d'éviter un conflit avec le collecteur de données de l'Agent WebSphere Applications.

Pourquoi et quand exécuter cette tâche

Il est possible que les types de collecteur de données suivants existent déjà dans le serveur d'applications qui doit être surveillé :

- Le collecteur de données de l'Agent WebSphere Applications, qui est installé dans une version antérieure d'IBM Cloud Application Performance Management
- Le collecteur de données de l'ITCAM Agent for WebSphere Applications, qui est installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring
- Tout autre collecteur de données qui n'est pas fourni par IBM

Procédure

Prenez les mesures appropriées afin d'éviter les conflits entre collecteurs de données.

- Pour une version antérieure du collecteur de données de l'Agent WebSphere Applications installée dans une version antérieure d'IBM Cloud Application Performance Management, vous avez les options suivantes :
  - Faites migrer le collecteur de données à l'aide de l'utilitaire de migration qui se trouve dans le répertoire de base du collecteur de données le plus récent. Pour plus d'informations, voir «Agent WebSphere Applications : migration du collecteur de données», à la page 982.
  - Annulez la configuration la version antérieure du collecteur de données, puis configurez à nouveau le collecteur de données à l'aide de l'utilitaire de configuration qui se trouve dans le répertoire de base du collecteur de données le plus récent. Pour plus d'informations sur l'annulation de la configuration du collecteur de données, voir «Agent WebSphere Applications : Annulation de la configuration du collecteur de données», à la page 189.
- Pour le collecteur de données de l'ITCAM Agent for WebSphere Applications, effectuez les étapes suivantes si vous voulez déployer la surveillance dans un environnement de coexistence des agents :
  1. Désinstallez le collecteur de données de l'ITCAM Agent for WebSphere Applications.
  2. Ne configurez qu'un seul collecteur de données pour envoyer les données à la fois à l'Agent WebSphere Applications et à l'ITCAM Agent for WebSphere Applications. Pour plus d'informations, voir «(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données», à la page 792.
- Pour les autres collecteurs de données non fournis par IBM, évaluez s'il est nécessaire de les supprimer. Le collecteur de données de l'Agent WebSphere Applications utilise la manipulation du code d'octet Java pour collecter les données. Les autres collecteurs de données qui utilisent la même méthode de collecte des données peuvent être en conflit avec le collecteur de données de l'Agent WebSphere Applications.

Configuration du collecteur de données avec l'utilitaire de configuration simple

L'Agent WebSphere Applications démarre automatiquement après l'installation, mais vous devez configurer manuellement le collecteur de données, un composant de l'agent, pour surveiller des instances de serveur d'applications.

Avant de commencer

- Assurez-vous que les exigences relatives à l'accès utilisateur sont remplies dans votre environnement. Pour plus d'informations, voir «Vérification des exigences d'accès utilisateur», à la page 769.
- Si un autre collecteur de données existe dans le serveur d'applications qui doit être surveillé, prenez les mesures appropriées afin d'éviter des conflits entre collecteurs de données. Pour plus d'informations, voir «Gestion d'un autre collecteur de données existant dans le serveur d'applications», à la page 770.

Pourquoi et quand exécuter cette tâche

Important :

- Si vous souhaitez configurer le collecteur de données pour la surveillance de ressources uniquement ou pour définir des options supplémentaires, utilisez la procédure de configuration complète. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.
- Si vous souhaitez modifier le nom du serveur dans l'interface utilisateur de surveillance, reconfigurez le collecteur de données et indiquez un alias de serveur. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.

Pour l'Agent WebSphere Applications, les variables *base_cd* font référence au répertoire de base du collecteur de données. L'emplacement de la variable *rép_base_cd* sur chaque système d'exploitation est le suivant :

- Windows *rép_install*\dchome\7.3.0.14.06
- Linux AIX *rép_install*/yndchome/7.3.0.14.06

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire `bin` au sein du répertoire de base du collecteur de données.
   - Windows *rép_install*\dchome\7.3.0.14.06\bin
   - Linux AIX *rép_install*/yndchome/7.3.0.14.06/bin
3. Exécutez l'utilitaire de configuration simple suivant:
   - Windows `simpleconfig.bat`
   - Linux AIX `./simpleconfig.sh`

   L'utilitaire **simpleconfig** reconnaît automatiquement les répertoires de base des serveurs d'applications.
4. Suivez les invites pour continuer la configuration du collecteur de données.

   Vous êtes tenu d'effectuer les actions suivantes selon les paramètres du serveur d'applications :
   - Pour un WebSphere Application Server traditionnel :
     - Sélectionnez le répertoire d'installation WebSphere découvert automatiquement ou indiquez-le manuellement.
     - Sélectionnez le profil WebSphere Application Server à surveiller.
     - Sélectionnez le profil des propriétés de sécurité à utiliser ou fournissez le nom d'utilisateur et le mot de passe de la console d'administration WebSphere (si la sécurité est activée pour le serveur d'applications).

- Pour WebSphere Application Server Liberty :
  - Indiquez le chemin d'accès complet du répertoire de base Liberty qui contient les répertoires `bin` et `servers` (par exemple, `/opt/ibm/wlp`).
  - Indiquez le répertoire de base du JRE qui est utilisé par Liberty.

5. Si possible, redémarrez l'instance de serveur d'applications une fois que la configuration du collecteur de données est terminée.
   a. Accédez au répertoire `bin` situé sous le répertoire de base du profil de serveur d'applications. Par exemple, `opt/IBM/WebSphere/AppServer/profiles/nom_profil/bin`.
   b. Arrêtez le serveur d'applications en entrant la commande **stopServer** dans la console de commande.
      - Linux AIX `./stopServer.sh nom_serveur`
      - Windows `stopServer.bat nom_serveur`
   c. A l'invite, entrez l'ID utilisateur et le mot de passe de l'administrateur de la console d'administration WebSphere.
   d. Redémarrez le serveur d'applications en entrant la commande **startServer** dans la console de commande.
      - Linux AIX `./startServer.sh nom_serveur`
      - Windows `startServer.bat nom_serveur`

Résultats

- Le collecteur de données est configuré pour surveiller toutes les instances d'un profil ou, dans le cas de WebSphere Application Server Liberty, une instance unique ou plusieurs instances dans le même répertoire. Pour surveiller plusieurs profils ou instances, répétez la configuration.
- Il est configuré dans les instances de serveur, fournissant ainsi un niveau de surveillance maximal.
- Pour Cloud APM, Base Private, la surveillance des ressources est activée.
- Pour Cloud APM, Advanced Private, la surveillance des ressources, le suivi des transactions et les données de diagnostic sont activés.

Limitation connue : Lors de la surveillance de WebSphere Application Server Liberty, le collecteur de données ne peut pas générer d'événements JNDI (Java Naming and Directory Interface),

Que faire ensuite

- Connectez-vous à la console Cloud APM et utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillée au Tableau de bord d'Application Performance. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

  A faire : Si l'Agent WebSphere Applications est configuré pour surveiller WebSphere Portal Server, il est lié au composant d'application WebSphere Portal Server dans le Tableau de bord d'Application Performance, pas à WebSphere Application Server.
- Si l'interface utilisateur de surveillance de la Tableau de bord d'Application Performance ne fournit pas d'informations sur l'instance de serveur d'applications, redémarrez le composant agent de surveillance de l'Agent WebSphere Applications en procédant comme suit :
  - Windows

    ```
    cd rép_install\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

```
cd rép_install/bin
./was-agent.sh
stop
./was-agent.sh start
```

Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète

Si vous souhaitez définir des options de configuration supplémentaires, vous pouvez utiliser les utilitaires de configuration complète (en mode interactif ou silencieux) pour configurer le collecteur de données plutôt que l'utilitaire de configuration simple. Vous pouvez également utiliser ces utilitaires de configuration complète pour reconfigurer le collecteur de données déjà configuré. En outre, vous devez utiliser l'utilitaire de configuration complète pour configurer la surveillance pour les instances WebSphere Portal Server.

Avant de commencer

- Assurez-vous que les exigences relatives à l'accès utilisateur sont remplies dans votre environnement. Pour plus d'informations, voir «Vérification des exigences d'accès utilisateur», à la page 769.
- Si un autre collecteur de données existe dans le serveur d'applications qui doit être surveillé, prenez les mesures appropriées afin d'éviter des conflits entre collecteurs de données. Pour plus d'informations, voir «Gestion d'un autre collecteur de données existant dans le serveur d'applications», à la page 770.

Pourquoi et quand exécuter cette tâche

Les utilitaires de configuration et de reconfiguration se trouvent dans les répertoires suivants :

- Windows *rép_install*\dchome\7.3.0.14.06\bin
- Linux AIX *rép_install*/yndchome/7.3.0.14.06/bin

Procédure

- L'utilitaire de configuration se nomme **config**. La configuration du collecteur de données avec l'utilitaire de configuration complète peut s'avérer nécessaire dans les cas suivants :
  - L'utilitaire de configuration **simpleconfig** échoue.
  - Vous souhaitez configurer la surveillance pour les instances WebSphere Portal Server.
  - Vous souhaitez indiquer un alias de serveur qui s'affiche dans l'interface utilisateur de surveillance pendant la configuration du collecteur de données.
  - Vous souhaitez disposer d'un contrôle plus précis des données à collecter. Par exemple, vous voulez n'utiliser que la surveillance des ressources et désactiver le suivi des données de diagnostics et des transactions.
  - Vous ne voulez pas configurer tous les serveurs d'applications en même temps dans le même profil.
  - Le collecteur de données n'est pas configuré dans le serveur d'applications et vous souhaitez le reconfigurer.

  Pour plus d'informations sur l'utilitaire de configuration complète interactive, voir «Configuration du collecteur de données en mode interactif», à la page 774.
- L'utilitaire de reconfiguration se nomme **reconfig**. La reconfiguration du collecteur de données peut s'avérer nécessaire dans les cas suivants :
  - Vous voulez reconfigurer le collecteur de données après qu'il a été configuré en mode interactif ou en mode silencieux.

  Pour plus d'informations sur l'utilitaire de reconfiguration interactive, voir «Reconfiguration du collecteur de données en mode interactif», à la page 778.
- Pour une configuration en mode silencieux, voir «Configuration du collecteur de données en mode silencieux», à la page 782.

Configuration du collecteur de données en mode interactif :

Utilisez l'utilitaire de configuration interactif (`config.sh` ou `config.bat`) pour configurer le collecteur de données lorsque l'utilitaire `simpleconfig` échoue. Vous pouvez utiliser l'utilitaire `config.sh` ou `config.bat` pour configurer le collecteur de données pour chaque instance de serveur d'applications que vous voulez surveiller.

Avant de commencer

Si vous configurez le collecteur de données pour surveiller WebSphere Application Server Liberty, définissez la variable d'environnement système **`JAVA_HOME`** sur la même machine JVM que celle utilisée pour le serveur d'applications. Par exemple, sur un système Windows, associez **`JAVA_HOME`** à la valeur `C:\Program Files\IBM\java`. Sur un système Linux, exécutez `export JAVA_HOME=/opt/IBM/java`.

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire de configuration complète pour configurer le collecteur de données :

- Windows *rép_install*`\dchome\7.3.0.14.06\bin\config.bat`
- Linux AIX *rép_install*`/yndchome/7.3.0.14.06/bin/config.sh`

Procédure

Pour reconfigurer le collecteur de données en répondant aux invites, procédez comme suit :

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire `bin` situé dans le répertoire de base du collecteur de données *base_cd*.
3. Démarrez l'utilitaire de configuration à l'aide de la commande suivante :
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   L'utilitaire de configuration affiche les adresses IP et les noms d'hôte de toutes les cartes réseau qui sont détectées sur le système informatique local.
4. Entrez le nombre qui correspond à l'adresse IP et au nom d'hôte. Si l'adresse IP et le nom d'hôte que vous voulez utiliser ne figurent pas dans la liste, entrez l'adresse IP ou le nom d'hôte.
5. Indiquez le répertoire de base du serveur d'applications qui doit être surveillé.
   - Pour un serveur WebSphere Application Server traditionnel, entrez le nombre qui correspond à un répertoire de base de serveur d'applications reconnu automatiquement, ou indiquez le chemin d'accès complet d'un répertoire de base de serveur d'applications.
   - Pour WebSphere Application Server Liberty, entrez le chemin d'accès complet au répertoire de base de WebSphere Application Server Liberty qui contient les répertoires `bin` et `servers`, par exemple `/opt/ibm/wlp`.
6. Si vous configurez le collecteur de données pour WebSphere Application Server Liberty, vous êtes invité à indiquer le répertoire de base Java. Indiquez le répertoire de base Java qui est utilisé pour le serveur d'applications. Par exemple, `/opt/IBM/java`.
7. Lorsque l'utilitaire de configuration répertorie tous les profils sous le répertoire de base du serveur d'applications spécifié, entrez le nombre qui correspond au profil du serveur d'applications que vous souhaitez configurer.
   - Pour un serveur WebSphere Application Server traditionnel, l'utilitaire de configuration indique ensuite si WebSphere Global Security est activé pour le profil WebSphere Application Server que vous avez spécifié. Si la sécurité globale n'est pas activée, passez à l'étape 9, à la page 775.
   - Pour WebSphere Application Server Liberty, passez à l'étape 10, à la page 775.
8. Si la sécurité globale n'est pas activée pour le profil WebSphere Application Server, indiquez s'il faut récupérer les paramètres de sécurité dans le fichier de propriétés d'un client. Entrez 1 pour permettre

à l'utilitaire de configuration d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié. Sinon, entrez 2 pour entrer le nom d'utilisateur et le mot de passe.

Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP. Si la sécurité globale est activée pour un profil de serveur d'applications, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à la console d'administration de WebSphere Application Server pour ce profil. Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI, ou le fichier `soap.client.props` pour une connexion SOAP.

9. Lorsque vous êtes invité à entrer le nom d'hôte de la console d'administration WebSphere, appuyez sur Entrée pour accepter les valeurs par défaut ou indiquez le nom d'hôte ou l'adresse IP de la console d'administration WebSphere. La valeur par défaut est `localhost`.

   A faire : Pour un environnement de déploiement réseau, entrez le nom d'hôte ou l'adresse IP de Deployment Manager.

10. Lorsque l'utilitaire de configuration affiche une liste de toutes les instances de serveur qui ne sont pas encore configurées pour la collecte de données, sélectionnez une ou plusieurs instances de serveur d'applications dans la liste. Entrez le nombre qui correspond à l'instance de serveur d'applications à configurer pour la collecte de données ou entrez un astérisque (*) pour configurer toutes les instances de serveur d'applications pour la collecte de données. Pour spécifier un sous-ensemble de serveurs, entrez les numéros qui représentent les serveurs, séparés par des virgules. Par exemple, `1,2,3`.

    A faire :

    - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration. (Une instance de WebSphere Application Server Liberty n'a pas besoin d'être en cours d'exécution).
    - Pour un environnement de déploiement réseau, Deployment Manager doit être en cours d'exécution.
    - Assurez-vous que les instances de serveur d'applications que vous sélectionnez sont les serveurs réels qui hébergent les applications ou les services que vous voulez surveiller.

11. Dans la section **Integration with Agent for WebSphere Applications**, indiquez si vous souhaitez intégrer le collecteur de données à l'Agent WebSphere Applications. Vous devez entrer 1 pour sélectionner cette option d'intégration, puis appuyer sur Entrée. Le serveur sélectionné sera enregistré pour la surveillance des ressources PMI.
12. Si vous configurez le collecteur de données pour un serveur WebSphere Application Server traditionnel, indiquez si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications.
    - Entrez 1 pour configurer le collecteur de données dans le serveur d'applications. Avec cette option, le collecteur de données est intégré au serveur d'applications, ce qui est nécessaire à la collecte complète des données de surveillance opérationnelle et de diagnostic. Cependant, la configuration du collecteur de données dans le serveur d'applications nécessite de redémarrer ce dernier. En outre, le collecteur de données peut affecter les performances de serveur.
    - Entrez 2 pour ne pas configurer le collecteur de données dans le serveur d'applications et passez à l'étape 14. Avec cette option, le collecteur de données s'exécute comme un processus autonome et seule la surveillance des ressources peut être activée.
13. A l'invite, indiquez s'il faut activer ou non le collecteur de données pour les données de diagnostic. Entrez 1 pour activer la collecte des données de diagnostic. La valeur par défaut est 2.
14. Lorsque vous êtes invité à entrer le nom d'hôte de l'agent de surveillance V8, entrez le nom d'hôte ou l'adresse IP de l'Agent WebSphere Applications ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut correspond au choix que vous avez effectué à l'étape 3.

L'agent de surveillance V8 fait référence à l'Agent WebSphere Applications, qui est installé avec IBM Cloud Application Performance Management.

15. Lorsque vous êtes invité à entrer le numéro de port de l'agent de surveillance V8, entrez le numéro de port de l'Agent WebSphere Applications ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut est `63335`.
16. Lorsque vous êtes invité à indiquer si l'agent de surveillance V6 pour WebSphere Applications doit être configuré, appuyez sur Entrée pour accepter la valeur par défaut No.

    L'agent de surveillance V6 fait référence à l'ITCAM Agent for WebSphere Applications, qui est installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring. La configuration de l'agent de surveillance V6 n'est requise que pour l'environnement de coexistence des agents.
17. Lorsque vous êtes invité à entrer l'alias de serveur, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre alias. Si vous configurez plusieurs instances de serveur d'applications, l'utilitaire de configuration vous invite à indiquer un alias pour chaque instance.

    Important : L'alias ne peut contenir que les caractères suivants : `A-Z`, `a-z`, soulignement (`_`), tiret (`-`) et point (`.`). N'utilisez pas d'autres caractères dans l'alias.

    L'alias de serveur est le premier qualificateur du nom d'instance d'agent (également appelé MSN) affiché sur la console Cloud APM. La valeur par défaut est le nom du noeud combiné au nom du serveur. Par exemple, l'alias **node1server1** indique le serveur **server1** dans le noeud **node1**.
18. Lorsque vous êtes invité à entrer un numéro de port pour la surveillance des ressources PMI, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un nouveau numéro. La valeur par défaut est `63355`.

    Ce port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Si le port par défaut est utilisé, vous pouvez définir un numéro différent.
19. Dans la section **Prise en charge du suivi des transactions**, indiquez si vous souhaitez activer le suivi des transactions. Entrez `1` pour activer la prise en charge du suivi des transactions. Autrement, entrez `2` et passez à l'étape 22.
20. Lorsque vous êtes invité à indiquer le nom d'hôte ou l'adresse IP de Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre nom d'hôte ou une autre adresse IP.

    Transaction Framework Extension est un composant interne de l'Agent WebSphere Applications qui recueille des mesures à partir du collecteur de données.
21. Lorsque vous êtes invité à entrer le numéro de port que le collecteur de données utilise pour se connecter à Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre numéro de port. La valeur par défaut est `5457`.
22. Indiquez si vous voulez intégrer le collecteur de données à Application Performance Diagnostics Lite. Appuyez sur Entrée pour accepter la valeur par défaut pour Non.
23. Dans la section **Paramètres avancés**, indiquez si vous souhaitez modifier le chemin du journal de la récupération de place. Entrez `1` pour sélectionner un chemin d'accès au journal de récupération de place. Autrement, entrez `2` et passez à l'étape 25, à la page 777. Pour utiliser le chemin d'accès au journal déjà indiqué dans l'argument JVM du serveur d'applications, entrez `2`.
24. Indiquez le chemin de la collecte de récupération de place. Entrez un nom de fichier avec son chemin d'accès complet. Pour WebSphere Application Server Liberty, n'utilisez pas de variables dans le chemin d'accès. Le collecteur de données modifie automatiquement le nom du fichier journal en y ajoutant des informations sur l'instance de serveur.

    Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *`nom_profil`*`.`*`nom-cellule`*`.`*`nom_noeud`*`.`*`nom_serveur`*`.gc.log` pour chaque instance de serveur d'applications configurée.

    Important : Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que `%pid`.

25. Consultez le récapitulatif de la configuration du collecteur de données à appliquer aux instances de serveur d'applications définies. Reconfigurez les parties de la configuration du collecteur de données avant d'appliquer les modifications, si nécessaire.
26. Entrez `a` pour accepter vos modifications.
27. A l'invite, indiquez si vous souhaitez créer une copie de sauvegarde de votre configuration en cours. Entrez 1 pour créer une sauvegarde de la configuration en cours. Sinon, entrez 2. L'utilitaire de configuration applique les modifications et présente un message d'état pour indiquer que la configuration du collecteur de données pour le profil est terminée .
28. Si vous configurez le collecteur de données pour le serveur WebSphere Application Server traditionnel, redémarrez les instances de serveur d'applications ou redémarrez l'agent, selon l'option que vous avez choisie à l'étape 12, à la page 775.
    - Si vous avez activé le collecteur de données dans le serveur d'applications, redémarrez les instances de serveur d'applications, comme indiqué par l'utilitaire de configuration.
    - Si vous avez activé la surveillance des ressources PMI sans activer le collecteur de données dans le serveur d'applications, redémarrez l'Agent WebSphere Applications en exécutant les commandes suivantes :
      – Windows
      ```
      cd rép_install\bin
      was-agent.bat stop
      was-agent.bat start
      ```
      – Linux AIX
      ```
      cd rép_install/bin
      ./was-agent.sh
      stop
      ./was-agent.sh start
      ```

    La configuration du collecteur de données entre en vigueur une fois que le serveur d'applications ou l'agent a redémarré.
29. Connectez-vous à la console Cloud APM pour afficher les données dans les tableaux de bord.
    a. Ouvrez une fenêtre de navigateur et entrez l'adresse URL suivante, où *hôte_serveur* correspond à l'adresse IP du serveur :

       `https://hôte_serveur:9443`
    b. Lorsque vous êtes invité à indiquer votre ID de connexion, entrez les données d'identification suivantes pour l'utilisateur par défaut ou entrez les données d'identification qui ont été affectées à votre administrateur de console Cloud APM :
       - Nom d'utilisateur : *apmadmin*
       - Mot de passe : *apmpass*

       Les données d'identification utilisateur initiales après l'installation du serveur Cloud APM sont `apmadmin` avec le mot de passe `apmpass`.
    c. Utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillé au Tableau de bord d'Application Performance. Vous pouvez l'ajouter en tant que nouveau composant à votre application existante ou créer une application à laquelle ajouter ce composant. Pour plus d'informations sur l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

Que faire ensuite

- Si l'ID utilisateur actuel utilisé pour configurer le collecteur de données n'est pas identique à l'ID de l'utilisateur qui exécute le serveur d'applications, vérifiez que l'ID utilisateur de configuration du collecteur de données dispose des droits en lecture et en écriture sur les répertoires `runtime` et `logs` dans le répertoire de base du collecteur de données. Ces deux sous-répertoires sont créés par l'ID de l'utilisateur qui exécute le serveur d'applications lorsque le serveur est redémarré.

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance dans les tableaux de bord. Si les données de surveillance ne sont pas disponibles immédiatement, redémarrez l'Agent WebSphere Applications en exécutant les commandes suivantes :
  - Windows
    ```
    cd rép_install\bin
    was-agent.bat stop
    was-agent.bat start
    ```
  - Linux AIX
    ```
    cd rép_install/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```
- La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si ce n'est pas la première fois que vous configurez le collecteur de données et que vous avez modifié l'alias de serveur, vous devez vider certains fichiers cache en effectuant les opérations suivantes :
  1. Arrêtez l'agent de surveillance s'il est en cours d'exécution.
  2. Ouvrez le fichier *nom_hôte*_yn.xml dans le répertoire suivant avec un éditeur de texte, où *nom_hôte* est le nom de l'hôte où l'Agent WebSphere Applications est installé.
     - Windows *rép_install*\TMAITM6_x64 (la valeur par défaut est C:\IBM\APM\TMAITM6_x64)
     - Linux AIX *rép_install*/config (la valeur par défaut est /opt/ibm/apm/agent/config)
  3. Recherchez la ligne qui commence par la chaîne suivante et qui contient le nom de serveur précédent. Par exemple, was85.win4net01Cell02.win4net01Node02.AppSrv01.server1, où server1 est le nom précédent du serveur d'applications.
     ```
     <!ENTITY code_produit_was.nom_cellule.nom_noeud.nom_profil.nom_serveur
     ```
     où *code_produit_was* est le code produit de WebSphere Application Server ; *nom_cellule* est le nom de la cellule ; *nom_noeud* est le nom du noeud ; *nom_profil* est le nom du profil de serveur d'applications ; *nom_serveur* est le nom précédent du serveur d'applications.
  4. Dans le répertoire en cours, recherchez le fichier .XML indiqué sur la ligne et supprimez-le.
  5. Supprimez la ligne que vous avez recherchée à l'étape 3 dans le fichier *nomhôte*_yn.xml.
  6. A la fin du fichier *nom_hôte*_yn.xml, supprimez la ligne qui contient les noms de serveur précédents.
  7. Sauvegardez et fermez le fichier.
  8. Redémarrez l'agent de surveillance.

Reconfiguration du collecteur de données en mode interactif :

Si vous avez configuré le collecteur de données pour surveiller une ou plusieurs instances de serveur d'applications, vous pouvez le reconfigurer à l'aide de l'utilitaire de reconfiguration (reconfig.sh ou reconfig.bat).

Avant de commencer

Si vous configurez le collecteur de données pour surveiller WebSphere Application Server Liberty, définissez la variable d'environnement système **JAVA_HOME** sur la même machine JVM que celle utilisée pour le serveur d'applications. Par exemple, sur un système Windows, associez **JAVA_HOME** à la valeur C:\Program Files\IBM\java. Sur un système Linux, exécutez export JAVA_HOME=/opt/IBM/java.

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire de reconfiguration complète pour configurer le collecteur de données :

- Windows *rép_install*\dchome\7.3.0.14.06\bin\reconfig.bat
- Linux AIX *rép_install*/yndchome/7.3.0.14.06/bin/reconfig.sh

A faire : L'utilitaire **reconfig** n'est pas applicable dans les cas suivants. A la place, utilisez l'utilitaire de configuration **config**. Bien que cet utilitaire vous avertisse que le serveur est déjà configuré, il peut toujours effectuer toutes les modifications souhaitées.

- Le collecteur de données est déjà configuré pour la surveillance des ressources uniquement et vous voulez le reconfigurer.
- Vous voulez reconfigurer le collecteur de données pour WebSphere Portal Server.

Conseil : Dans les invites vous invitant à définir les paramètres de configuration de l'agent, l'utilitaire de reconfiguration propose les valeurs actuellement configurées comme valeurs par défaut.

Procédure

Pour reconfigurer le collecteur de données en répondant aux invites, procédez comme suit :

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire `bin` situé dans le répertoire de base du collecteur de données *base_cd*.
3. Démarrez l'utilitaire de reconfiguration à l'aide de la commande suivante :
   - Windows `reconfig.bat`
   - Linux AIX `./reconfig.sh`

   Conseil : L'exécution de cet utilitaire de reconfiguration a le même effet que l'exécution du script `config.bat` avec l'argument `-reconfig` sur les systèmes Windows, ou le script `config.sh` avec l'argument `-reconfig` sur les systèmes Linux et AIX.
   L'utilitaire de reconfiguration affiche les adresses IP de toutes les cartes réseau qui sont détectées sur le système informatique local.
4. Entrez le nombre qui correspond à l'adresse IP à utiliser. L'utilitaire de reconfiguration recherche toutes les instances de serveur d'applications pour lesquelles le collecteur de données est configuré sur cet hôte et vous invite à sélectionner une ou plusieurs instances de serveur d'applications dans la liste.
5. Sélectionnez une ou plusieurs instances de serveur d'applications dans la liste. Entrez le nombre qui correspond à l'instance de serveur d'applications à reconfigurer pour la collecte de données ou entrez un astérisque (`*`) pour reconfigurer toutes les instances de serveur d'applications pour la collecte de données. Pour indiquer un sous-ensemble de serveurs, entrez les nombres, séparés par des virgules, qui représentent les serveurs. Par exemple : `1,2,3`.

   A faire :
   - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration. (Une instance de WebSphere Application Server Liberty n'a pas besoin d'être en cours d'exécution).
   - Pour un environnement de déploiement réseau, Deployment Manager doit être en cours d'exécution.
   - Assurez-vous que les instances de serveur d'applications que vous sélectionnez sont les serveurs réels qui hébergent les applications ou les services que vous voulez surveiller.
6. Dans la section **Integration with Agent for WebSphere Applications**, indiquez si vous souhaitez intégrer le collecteur de données à l'Agent WebSphere Applications. Vous devez entrer 1 pour sélectionner cette option d'intégration, puis appuyer sur Entrée.

7. Si vous configurez le collecteur de données pour un serveur WebSphere Application Server traditionnel, indiquez si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications.
   - Entrez 1 pour configurer le collecteur de données dans le serveur d'applications. Avec cette option, le collecteur de données est intégré au serveur d'applications, ce qui est nécessaire à la collecte complète des données de surveillance opérationnelle et de diagnostic. Cependant, la configuration du collecteur de données dans le serveur d'applications nécessite de redémarrer ce dernier. En outre, le collecteur de données peut affecter les performances de serveur.
   - Entrez 2 pour ne pas configurer le collecteur de données dans le serveur d'applications et passez à l'étape 9. Avec cette option, le collecteur de données s'exécute comme un processus autonome et seule la surveillance des ressources PMI peut être activée.
8. A l'invite, indiquez s'il faut activer ou non la collecte des données de diagnostic pour le collecteur de données. Entrez 1 pour oui ou 2 pour non.
9. Lorsque vous êtes invité à entrer le nom d'hôte, entrez le nom d'hôte ou l'adresse IP de l'Agent WebSphere Applications ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut correspond au choix que vous avez effectué à l'étape 4, à la page 779.
10. Lorsque vous êtes invité à entrer le numéro de port, entrez le numéro de port de l'agent de surveillance ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut est 63335.
11. Lorsque vous êtes invité à indiquer si l'agent de surveillance V6 pour WebSphere Applications doit être configuré, appuyez sur Entrée pour accepter la valeur par défaut No.

    L'agent de surveillance V6 fait référence à l'ITCAM Agent for WebSphere Applications, qui est installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring. La configuration de l'agent de surveillance V6 n'est requise que pour l'environnement de coexistence des agents.
12. Lorsque vous êtes invité à entrer l'alias de serveur, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre alias. Si vous configurez plusieurs instances de serveur d'applications, l'utilitaire de configuration vous invite à indiquer un alias pour chaque instance.

    Important : L'alias ne peut contenir que les caractères suivants : A-Z, a-z, soulignement (_), tiret (-) et point (.). N'utilisez pas d'autres caractères dans l'alias.

    L'alias de serveur est le premier qualificateur du nom d'instance d'agent (également appelé MSN) affiché sur la console Cloud APM. La valeur par défaut est le nom du noeud combiné au nom du serveur. Par exemple, l'alias **node1server1** indique le serveur **server1** dans le noeud **node1**.
13. Lorsque vous êtes invité à entrer un numéro de port pour la surveillance des ressources PMI, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un nouveau numéro. La valeur par défaut est 63355.

    Ce port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Si le port par défaut est utilisé, vous pouvez définir un numéro différent.
14. Dans la section **Prise en charge du suivi des transactions**, indiquez si vous souhaitez activer le suivi des transactions. Entrez 1 pour activer la prise en charge du suivi des transactions. Autrement, entrez 2 et passez à l'étape 17.
15. Lorsque vous êtes invité à indiquer le nom d'hôte ou l'adresse IP de Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre nom d'hôte ou une autre adresse IP.

    Transaction Framework Extension est un composant interne de l'Agent WebSphere Applications qui recueille des mesures à partir du collecteur de données.
16. Lorsque vous êtes invité à entrer le numéro de port que le collecteur de données utilise pour se connecter à Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre numéro de port. La valeur par défaut est 5457.
17. Indiquez si vous voulez intégrer le collecteur de données à Application Performance Diagnostics Lite. Appuyez sur Entrée pour accepter la valeur par défaut pour Non.

18. Dans la section **Paramètres avancés**, indiquez si vous souhaitez modifier le chemin du journal de la récupération de place. Entrez 1 pour sélectionner un chemin d'accès au journal de récupération de place. Autrement, entrez 2 et passez à l'étape 20. Pour utiliser le chemin d'accès au journal déjà indiqué dans l'argument JVM du serveur d'applications, entrez 2.
19. Indiquez le chemin de la collecte de récupération de place. Entrez un nom de fichier avec son chemin d'accès complet. Pour WebSphere Application Server Liberty, n'utilisez pas de variables dans le chemin d'accès. Le collecteur de données modifie automatiquement le nom du fichier journal en y ajoutant des informations sur l'instance de serveur.

    Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *nom_profil*`.`*nom-cellule*`.`*nom_noeud*`.`*nom_serveur*`.gc.log` pour chaque instance de serveur d'applications configurée.

    Important : Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que `%pid`.
20. Consultez le récapitulatif de la configuration du collecteur de données à appliquer aux instances de serveur d'applications définies. Reconfigurez les parties de la configuration du collecteur de données avant d'appliquer les modifications, si nécessaire.
21. Entrez `a` pour accepter vos modifications.
22. A l'invite, indiquez si vous souhaitez créer une copie de sauvegarde de votre configuration en cours. Entrez 1 pour créer une sauvegarde de la configuration en cours. Sinon, entrez 2. L'utilitaire de configuration applique les modifications et présente un message d'état pour indiquer que la configuration du collecteur de données pour le profil est terminée .
23. Si vous configurez le collecteur de données pour le serveur WebSphere Application Server traditionnel, redémarrez les instances de serveur d'applications ou redémarrez l'agent, selon l'option que vous avez choisie à l'étape 7, à la page 780.
    - Si vous avez activé le collecteur de données dans le serveur d'applications, redémarrez les instances de serveur d'applications, comme indiqué par l'utilitaire de configuration.
    - Si vous avez activé la surveillance des ressources PMI sans activer le collecteur de données dans le serveur d'applications, redémarrez l'Agent WebSphere Applications en exécutant les commandes suivantes :
      – Windows
      ```
      cd rép_install\bin
      was-agent.bat stop
      was-agent.bat start
      ```
      – Linux AIX
      ```
      cd rép_install/bin
      ./was-agent.sh stop
      ./was-agent.sh start
      ```

    La configuration du collecteur de données entre en vigueur une fois que le serveur d'applications ou l'agent a redémarré.

Que faire ensuite

- La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si vous avez modifié l'alias de serveur lors de la procédure de reconfiguration, vous devez effacer certains fichiers cache en effectuant les opérations suivantes :
  1. Arrêtez l'agent de surveillance s'il est en cours d'exécution.
  2. Ouvrez le fichier *nom_hôte*`_yn.xml` dans le répertoire suivant avec un éditeur de texte, où *nom_hôte* est le nom de l'hôte où l'Agent WebSphere Applications est installé.
     – Windows *rép_install*`\TMAITM6_x64` (la valeur par défaut est `C:\IBM\APM\TMAITM6_x64`)
     – Linux AIX *rép_install*`/config` (la valeur par défaut est `/opt/ibm/apm/agent/config`)

3. Recherchez la ligne qui commence par la chaîne suivante et qui contient le nom de serveur précédent. Par exemple, `was85.win4net01Cell02.win4net01Node02.AppSrv01.server1`, où `server1` est le nom précédent du serveur d'applications.

   ```
   <!ENTITY code_produit_was.nom_cellule.nom_noeud.nom_profil.nom_serveur
   ```

   où *code_produit_was* est le code produit de WebSphere Application Server ; *nom_cellule* est le nom de la cellule ; *nom_noeud* est le nom du noeud ; *nom_profil* est le nom du profil de serveur d'applications ; *nom_serveur* est le nom précédent du serveur d'applications.
4. Dans le répertoire en cours, recherchez le fichier `.XML` indiqué sur la ligne et supprimez-le.
5. Supprimez la ligne que vous avez recherchée à l'étape 3 dans le fichier *nomhôte*`_yn.xml`.
6. A la fin du fichier *nom_hôte*`_yn.xml`, supprimez la ligne qui contient les noms de serveur précédents.
7. Sauvegardez et fermez le fichier.
8. Redémarrez l'agent de surveillance.

Configuration du collecteur de données en mode silencieux :

Si vous voulez configurer de nombreuses instances de serveur d'applications, il peut être plus pratique de configurer le collecteur de données en mode silencieux.

Pourquoi et quand exécuter cette tâche

Lorsque vous configurez le collecteur de données en mode silencieux, vous indiquez d'abord des options de configuration dans un fichier de propriétés. Un exemple de fichier de propriétés, `sample_silent_config.txt`, est fourni avec l'utilitaire de configuration. Le fichier est disponible dans les répertoires suivants, où *base_cd* est le répertoire dans lequel est installé le collecteur de données. Pour le chemin d'accès complet au répertoire *base_cd*, consultez l'introduction de Configuration du collecteur de données pour l'agent WebSphere Applications.

- Windows *base_cd*`\bin`
- Linux AIX *base_cd*`/bin`

Pour plus d'informations sur chaque propriété de configuration disponible dans ce fichier, voir «Fichier de propriétés pour la configuration en mode silencieux du collecteur de données», à la page 783.

Procédure

Exécutez les étapes suivantes pour effectuer une configuration en mode silencieux :

1. Spécifiez les options de configuration dans le fichier de propriétés. Vous pouvez copier l'exemple de fichier de propriétés et modifier les options obligatoires.
2. Définissez l'emplacement du répertoire principal Java avant d'exécuter l'utilitaire. Par exemple :
   - Windows
     ```
     set JAVA_HOME=C:\Program Files\IBM\WebSphere\AppServer80\java
     ```
   - Linux AIX
     ```
     export JAVA_HOME=/opt/IBM/AppServer80/java
     ```

   Important : Si vous configurez la surveillance pour WebSphere Application Server Liberty, vous devez utiliser la même version de machine JVM que celle utilisée pour le serveur d'applications. Autrement, la surveillance peut échouer.
3. Accédez au répertoire suivant :
   - Windows *base_cd*`\bin`
   - Linux AIX *base_cd*`/bin`

4. Exécutez la commande pour configurer le collecteur de donnés en mode silencieux.
   - Windows Exécutez la commande suivante comme administrateur ayant installé WebSphere Application Server.

     ```
     config.bat -silent [dir_path]\silent file
     ```

   - Linux AIX Exécutez la commande suivante avec les privilèges de superutilisateur.

     ```
     config.sh -silent [dir_path]/silent file
     ```

   Conseil : Si l'utilisateur `wsadmin` a été utilisé pour installer le serveur d'applications, exécutez l'utilitaire `config` en tant qu'utilisateur `wsadmin` ou avec les privilèges de superutilisateur.
5. Après avoir configuré le collecteur de données pour surveiller des instances de serveur d'applications, si vous avez activé le collecteur de données dans le serveur d'applications, vous devez redémarrer les instances. La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré.
6. Si vous avez activé la surveillance des ressources PMI sans avoir activé le collecteur de données dans le serveur d'applications, il se peut que vous deviez redémarrer l'Agent WebSphere Applications pour démarrer la surveillance. Si les données de surveillance ne sont pas disponibles immédiatement, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
   - Windows

     ```
     cd rép_install\bin
     was-agent.bat stop
     was-agent.bat start
     ```

   - Linux AIX

     ```
     cd rép_install/bin
     ./was-agent.sh stop
     ./was-agent.sh start
     ```

Que faire ensuite

Après une configuration en mode silencieux, pour modifier la configuration du collecteur de données, vous avez deux options :

- Reconfigurez-le de façon interactive à l'aide de l'utilitaire de reconfiguration **reconfig**. Pour plus d'informations, voir «Reconfiguration du collecteur de données en mode interactif», à la page 778.
- Annulez la configuration en mode silencieux, puis utilisez la même procédure pour la configurer de nouveau en mode silencieux. Pour plus d'informations, voir «Annulation de la configuration du collecteur de données en mode silencieux», à la page 191.

Référence associée:

«Fichier de propriétés pour la configuration en mode silencieux du collecteur de données»
Pour configurer le collecteur de données en mode silencieux, vous indiquez des options de configuration dans un fichier de propriétés, puis vous exécutez l'utilitaire de configuration.

Fichier de propriétés pour la configuration en mode silencieux du collecteur de données :

Pour configurer le collecteur de données en mode silencieux, vous indiquez des options de configuration dans un fichier de propriétés, puis vous exécutez l'utilitaire de configuration.

Lorsque vous créez votre fichier de propriétés, tenez compte des remarques suivantes :

- Une ligne du fichier qui commence par un signe dièse (#) est considérée comme un commentaire et n'est pas traitée. Si le signe dièse est utilisé ailleurs dans la ligne, on ne le considère pas comme le début d'un commentaire.
- Chaque propriété est décrite sur une ligne distincte, dans le format suivant : *property* = *value*.

property
Nom de la propriété. La liste de propriétés valides que vous pouvez configurer est affichée dans le tableau 186.

value Valeur de la propriété. Des valeurs par défaut pour certaines propriétés sont déjà fournies. Vous pouvez supprimer des valeurs par défaut pour laisser des valeurs de propriété en blanc. Une valeur vide est traitée comme si la propriété n'était pas indiquée, par opposition à l'utilisation de la valeur par défaut. Si vous voulez utiliser des valeurs par défaut, vous pouvez mettre en commentaire la propriété dans le fichier.

- Les mots de passe sont en texte en clair.
- Les propriétés et leurs valeurs distinguent les majuscules et minuscules.

Le tableau 186 décrit les propriétés qui sont disponibles lors de la configuration du collecteur de données en mode silencieux.

Important : Si vous configurez le collecteur de données pour une instance de WebSphere Application Server Liberty, certaines des propriétés ne sont pas utilisées.

Tableau 186. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux.

Propriété	Commentaire
default.hostip	Si le système informatique utilise plusieurs adresses IP, indiquez l'adresse IP que le collecteur de données doit utiliser.
Intégration du collecteur de données au serveur de gestion d'ITCAM for Application Diagnostics **Important :** Le serveur de gestion est uniquement disponible si vous avez ITCAM for Application Diagnostics. Pour une instance WebSphere Application Server Liberty ou dans un environnement Cloud APM, ces propriétés ne sont pas utilisées.	
ms.connect	Indique si le collecteur de données est configuré pour se connecter au serveur de gestion dans un environnement ITCAM for Application Diagnostics. Les valeurs valides sont `True` et `False`.
ms.kernel.host	Indique le nom de système hôte qualifié complet du serveur de gestion.
ms.kernel.codebase.port	Indique le port de codebase sur lequel le serveur de gestion est en mode écoute.
ms.am.home	Indique le répertoire de base du serveur de gestion.
ms.am.socket.bindip	Indique l'adresse IP ou le nom d'hôte que le collecteur de données doit utiliser pour communiquer avec le serveur de gestion. Si plus d'une interface réseau ou adresse IP est configurée sur le système informatique du collecteur de données, sélectionnez l'une d'entre elles.
ms.probe.controller.rmi.port	Si le collecteur de données est derrière un pare-feu ou si vous avez des exigences particulières de modification du port RMI de contrôleur du collecteur de données, définissez cette plage de numéros de port. Configurez ce numéro de port comme autorisé par le pare-feu pour l'hôte du collecteur de données. Par exemple : `ms.probe.controller.rmi.port=8300-8399` ou ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	Si le collecteur de données est derrière un pare-feu ou si vous avez des exigences particulières de modification du port RMI du collecteur de données, définissez cette plage de numéros de port. Configurez ce numéro de port comme autorisé par le pare-feu pour l'hôte du collecteur de données. Par exemple : `ms.probe.rmi.port=8200-8299` ou `ms.probe.rmi.port=8200`.

Tableau 186. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite).

Propriété	Commentaire
Prise en charge du suivi des transactions Pour visualiser les informations de suivi des transactions, vous devez avoir des vues de topologie disponibles dans la console Cloud APM et activer le suivi des transactions dans la fenêtre de configuration de l'agent.	
ttapi.enable	Indique si le collecteur de données prend en charge le suivi des transactions. Les valeurs valides sont `True` et `False`.
ttapi.host	Indique l'hôte de Transaction Framework Extension, qui est le composant de l'agent de surveillance pour WebSphere Applications qui regroupe les mesures provenant du collecteur de données. Utilisez la valeur de l'hôte local, `127.0.0.1`.
ttapi.port	Indique le port de Transaction Framework Extension. Utilisez `5457`.
Intégration du collecteur de données à ITCAM for SOA **Important :** Pour une instance WebSphere Application Server Liberty ou dans un environnement Cloud APM, cette propriété n'est pas utilisée.	
soa.enable	Indique si vous souhaitez intégrer le collecteur de données à ITCAM for SOA. L'agent ITCAM for SOA doit être installé pour que vous puissiez terminer la configuration.
Intégration du collecteur de données à Tivoli Performance Monitoring **Important :** Pour une instance WebSphere Application Server Liberty ou dans un environnement Cloud APM, cette propriété n'est pas utilisée.	
tpv.enable	Indique si vous souhaitez intégrer le collecteur de données à Tivoli Performance Monitoring lorsque le collecteur de données est inclus en tant qu'élément d'ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring est accessible depuis la console d'administration de WebSphere Application Server. Les valeurs valides sont *True* et *False*.
Intégration du collecteur de données à Application Performance Diagnostics Lite **Important :** Pour une instance WebSphere Application Server Liberty, cette propriété n'est pas utilisée.	
de.enable	Indique s'il y a lieu de collecter des données de diagnostic qui sont requises pour Application Performance Diagnostics et Application Performance Diagnostics Lite. Les valeurs valides sont `True` et `False`. Activez cette intégration si vous disposez du produit Application Diagnostics ou si vous souhaitez l'acquérir ultérieurement. Dans ce cas, la collecte des données de diagnostic est activée au démarrage du serveur. Sinon, elle est désactivée au démarrage ; vous pouvez alors l'activer à l'aide de la page Configuration d'agent de l'interface utilisateur. Toutefois, si le serveur est redémarré, la collecte des données de diagnostic sera à nouveau désactivée. Ce paramètre active également l'intégration à Application Performance Diagnostics Lite, un outil conçu pour l'étude de diagnostic des applications exécutées sur WebSphere Application Server et WebSphere Portal Server. A l'aide de cet outil, vous pouvez analyser des données en temps réel ou vous pouvez sauvegarder les informations de diagnostic dans un fichier à des fins d'analyse ultérieure.
Surveillance des ressources PMI et du collecteur de données Le serveur sélectionné est toujours configuré pour la surveillance des ressources (PMI), sans aucun changement apporté au serveur d'applications. Cette option de surveillance fournit des mesures et des travaux limités seulement avec Agent WebSphere Applications, mais ne nécessite pas une relance du serveur d'application et ne peut pas affecter la performance.	

Tableau 186. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite).

Propriété	Commentaire
tema.appserver	Indique si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications. Le collecteur de données de l'instance de serveur d'application est nécessaire pour obtenir l'éventail complet de mesures dans l'Agent WebSphere Applications et pour l'intégration à tous les autres produits. Cependant, la configuration du collecteur de données nécessite le redémarrage du serveur d'applications. En outre, le collecteur de données peut affecter les performances de serveur. Les valeurs valides sont `True` et `False`. Si ce paramètre a pour valeur `False`, les paramètres de configuration du collecteur de données pour une intégration à des produits autres que l'Agent WebSphere Applications ne sont pas pris en compte. Lorsque ce paramètre est défini sur `False`, les fonctions de diagnostic et de suivi des transactions sont indisponibles, et seules les données de surveillance des ressources sont collectées.
tema.jmxport	Le numéro du port TCP/IP pour la surveillance des ressources. Le port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Le port de défaut est 63355 ; si ce port est utilisé, vous pouvez définir un numéro différent.
Intégration du collecteur de données à l'Agent WebSphere Applications et Application Performance Diagnostics Lite	
temaconnect	Indique si le collecteur de données se connecte au composant agent de surveillance de l'Agent WebSphere Applications. Les valeurs valides sont `True` et `False`. **Important :** Vous devez utiliser la valeur `True` pour utiliser l'Agent WebSphere Applications.
tema.appserver	Indique si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications. Le collecteur de données de l'instance de serveur d'application est nécessaire pour obtenir l'éventail complet de mesures dans l'Agent WebSphere Applications et pour l'intégration à tous les autres produits. Elle nécessite le redémarrage du serveur d'applications. En outre, le collecteur de données peut affecter les performances de serveur. Les valeurs valides sont `True` et `False`. Si ce paramètre est associé à la valeur `False`, les paramètres de configuration pour l'intégration du collecteur de données à des produits autres que l'Agent WebSphere Applications ne sont pas pris en compte, de même que les paramètres tema.host et tema.port suivants. Lorsque ce paramètre est défini sur `False`, les fonctions de diagnostic et de suivi des transactions sont indisponibles, et seules les données de surveillance des ressources sont collectées.
tema.host	Indique le nom d'hôte complet ou l'adresse IP du composant agent de surveillance de l'Agent WebSphere Applications. Utilisez l'adresse de l'hôte local (127.0.0.1).
tema.port	Indiquez le numéro de port du composant agent de surveillance de l'Agent WebSphere Applications. Ne modifiez pas la valeur par défaut 63335.
tema.jmxport	Le numéro du port TCP/IP pour la surveillance des ressources. Le port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Le port de défaut est 63355 ; si ce port est utilisé, vous pouvez définir un numéro différent.
Intégration du collecteur de données à ITCAM Agent for WebSphere Applications version 6 Utilisez les propriétés suivantes pour demander à un collecteur de données de collecter des données pour l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications version 6.	

Tableau 186. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite).

Propriété	Commentaire
config.tema.v6	Indique si le collecteur de données doit être intégré au composant agent de surveillance de l'ITCAM Agent for WebSphere Applications version 6. Les valeurs admises sont `True` et `False`. La valeur par défaut est `False`.
tema.host.v6	Indique si le collecteur de données doit être intégré au composant agent de surveillance de l'ITCAM Agent for WebSphere Applications version 6. Les valeurs admises sont `True` et `False`. La valeur par défaut est `False`.
tema.port.v6	Indique le numéro de port du composant agent de surveillance de l'ITCAM Agent for WebSphere Applications version 6. Ne modifiez pas la valeur par défaut 63336.
Sauvegarde de WebSphere Application Server	
was.backup.configuration	Indique si la configuration en cours de WebSphere Application Server doit être sauvegardée avant que la nouvelle configuration soit appliquée. Les valeurs valides sont `True` et `False`.
was.backup.configuration.dir	Indique l'emplacement du répertoire de sauvegarde.
Paramètres de configuration avancés	
was.gc.custom.path	Indique si vous devez définir un chemin d'accès personnalisé pour le journal de récupération de place.
was.gc.file	Indique le chemin d'accès au journal de récupération de place personnalisé. Définissez cette valeur sur un nom de fichier avec son chemin d'accès complet. Le collecteur de données modifie automatiquement le nom du fichier journal en y ajoutant des informations sur l'instance de serveur. Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *`nom_profil.nom-cellule.nom_noeud.nom_serveur`*`.gc.log` pour chaque instance de serveur d'applications configurée. **Important :** Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que %pid.
Paramètre de connexion de WebSphere Administrative Services	
was.wsadmin.connection.host	Indique le nom de l'hôte auquel l'outil wsadmin se connecte. Dans un environnement Network Deployment, spécifiez la connexion wsadmin au gestionnaire de déploiement. Dans un environnement autonome, indiquez la connexion wsadmin au serveur. **A faire :** Si la console d'administration WebSphere est sur le même système, la valeur de `localhost` est utilisée pour la connexion. Toutefois, dans certains cas, `localhost` n'est pas autorisé pour la communication en raison des paramètres de sécurité ou du réseau système. Dans ce cas, vous devez spécifier ce paramètre dans le fichier de réponses silencieux.
was.wsadmin.connection.type	Indique le port que l'outil wsadmin doit utiliser pour se connecter à WebSphere Application Server.
was.wsadmin.connection.port	Indique le port que l'outil wsadmin doit utiliser pour se connecter à WebSphere Application Server.
Paramètres de sécurité globale de WebSphere Application Server	
was.wsadmin.username	Spécifie l'ID utilisateur d'un utilisateur autorisé à se connecter à la console d'administration d'IBM WebSphere Application Server. Cet utilisateur doit posséder le rôle d'agent sur le serveur d'applications.
was.wsadmin.password	Indique le mot de passe qui correspond à l'utilisateur indiqué dans la propriété `was.wsadmin.username`.
was.client.props	Indique si les paramètres de sécurité doivent être extraits à partir d'un fichier de propriétés de client. Les valeurs valides sont `True` et `False`.
Paramètres de WebSphere Application Server	

Tableau 186. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite).

Propriété	Commentaire
was.appserver.profile.name	Indique le nom du profil de serveur d'applications que vous voulez configurer. Pas utilisé pour WebSphere Application Server Liberty.
was.appserver.home	Indique le répertoire de base de WebSphere Application Server.
was.appserver.cell.name	Indique le nom de cellule de WebSphere Application Server. Pas utilisé pour WebSphere Application Server Liberty.
was.appserver.node.name	Indique le nom de noeud de WebSphere Application Server. Pas utilisé pour WebSphere Application Server Liberty.
Paramètres de l'instance d'exécution de WebSphere Application Server	
was.appserver.server.name	Indique l'instance du serveur d'applications dans le profil de serveur d'applications à configurer. **Conseil :** • Le fichier de réponses silencieux peut avoir plusieurs instances de cette propriété • Lors de l'ajout d'un deuxième serveur, supprimez la mise en commentaire de ce dernier (#[SERVER]) et ajoutez le nom du serveur.
tema.serveralias	Spécifie le nom du noeud dans l'interface utilisateur de surveillance qui contient les informations de surveillance pour cette instance du serveur d'applications. La valeur par défaut est le nom du noeud combiné au nom du serveur. **Important :** L'alias ne peut contenir que les caractères suivants : `A-Z`, `a-z`, soulignement (_), tiret (`-`) et point (`.`). N'utilisez pas d'autres caractères dans l'alias. **Conseil :** Le fichier de réponses silencieux peut avoir plusieurs instances de cette propriété. **A faire :** La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si ce n'est pas la première fois que vous configurez le collecteur de données et que vous avez modifié l'alias de serveur, vous devez effacer certains fichiers cache. Pour plus d'instructions, voir la rubrique décrivant l'effacement des fichiers cache portant des anciens noms de serveur.

Configuration manuelle du collecteur de données si les utilitaires de configuration échouent

Si vous ne pouvez pas utiliser l'utilitaire de configuration fourni pour configurer le collecteur de données pour l'Agent WebSphere Applications, vous pouvez configurer manuellement le collecteur de données dans la console d'administration WebSphere.

Avant de commencer

- Installez l'Agent WebSphere Applications.
- Prenez connaissance du répertoire de base du collecteur de données, requis par la configuration du collecteur de données. Le répertoire par défaut est `/opt/ibm/apm/agent/yndchome/7.3.0.14.06` sur les systèmes Linux et AIX ou `C:\IBM\APM\dchome\7.3.0.14.06` sur les systèmes Windows.
- Si vous souhaitez configurer le collecteur de données pour un serveur Liberty, prenez connaissance du répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/was/liberty/usr/servers/defaultServer`.
- Assurez-vous qu'un fichier nommé `itcam_wsBundleMetaData.xml` existe dans le dossier *rép_principal_dc*`/runtime/wsBundleMetaData` et qu'il contient les informations suivantes. Si le dossier ou le fichier n'existe pas, créez-le manuellement.

  A faire : La valeur *rép_plugins_dans_rép_principal_dc* doit être définie sur le chemin d'accès absolu du dossier `plugins` dans le répertoire principal du collecteur de données. Le répertoire par défaut est

`/opt/ibm/apm/agent/yndchome/7.3.0.14.06/plugins` sur les systèmes Linux et AIX ou `C:\IBM\APM\dchome\7.3.0.14.06\plugins` sur les systèmes Windows.

```
<bundles>
  <directory path="rép_plugins_dans_rép_principal_dc">
      <bundle>com.ibm.tivoli.itcam.bundlemanager_7.2.0.jar</bundle>
  </directory>
  <directory path="rép_plugins_dans_rép_principal_dc">
      <bundle>com.ibm.tivoli.itcam.classicsca_7.2.0.jar</bundle>
  </directory>
  <directory path="rép_plugins_dans_rép_principal_dc">
      <bundle>com.ibm.tivoli.itcam.toolkitsca.classicsca_7.2.0.jar</bundle>
  </directory>
</bundles>
```

Pourquoi et quand exécuter cette tâche

Important :

- Vous devez apporter des modifications manuelles à la configuration WebSphere Application Server pour les collecteurs de données en tant qu'administrateur WebSphere.
- Vous devez être un administrateur WebSphere expérimenté pour apporter des modifications manuelles à WebSphere Application Server en vue de la collecte de données. Toute erreur dans la modification manuelle de la configuration peut empêcher le démarrage du serveur d'applications.
- Après avoir configuré manuellement le collecteur de données pour surveiller les instances de serveur d'application, vous ne pouvez pas employer l'utilitaire d'annulation de configuration pour déconfigurer le collecteur de données. Vous devez à la place annuler manuellement la configuration du collecteur de données.

Procédure

- Pour configurer manuellement le collecteur de données pour WebSphere Application Server, voir «Configuration manuelle du collecteur de données pour WebSphere Application Server traditionnel».
- Pour configurer manuellement le collecteur de données pour le serveur Liberty, voir «Configuration manuelle du collecteur de données pour WebSphere Application Server Liberty», à la page 791.

Configuration manuelle du collecteur de données pour WebSphere Application Server traditionnel : Procédure

1. Connectez-vous à la console d'administration WebSphere en tant qu'administrateur.
2. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Types** et cliquez sur **WebSphere application servers**.
3. Dans la section **Server Infrastructure** de l'onglet Configuration, développez **Gestion des processus et Java** et cliquez sur **Process Definition**.
4. Dans la section **Propriétés supplémentaires**, cliquez sur **Machine virtuelle Java**.
5. Dans la zone **Arguments JVM génériques**, ajoutez les entrées suivantes :

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
   toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
   etc/datacollector.policy -verbosegc
   ```

   Lors de l'ajout de ces entrées, notez ce qui suit :

   - Toutes les entrées doivent se trouver sur une seule ligne.
   - Séparez les différents arguments par des espaces avant le signe moins (-). N'utilisez pas d'espaces ailleurs.
6. Cliquez sur **Apply**, puis enregistrez les changements apportés à la configuration principale.
   - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
   - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné dans les **options de préférence de la console**, puis cliquez sur **Sauvegarder**.

7. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Types**, cliquez sur **WebSphere application servers**, puis cliquez sur le nom du serveur.
8. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
9. Selon le système d'exploitation, la plateforme matérielle et la machine virtuelle Java de serveur d'applications utilisés, définissez l'entrée d'environnement suivante.

Tableau 187. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/li6263`
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lx8266`
Linux sur Power Little Endian (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lpl266`
Linux sur System z (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3263`
Linux sur System z (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3266`
Windows (machine virtuelle Java 32 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win32`
Windows (machine virtuelle Java 64 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win64`

10. Cliquez sur **Apply**, puis enregistrez les changements apportés à la configuration principale.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné dans les **options de préférence de la console**, puis cliquez sur **Sauvegarder**.
11. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
12. Définissez la portée sur un niveau serveur approprié et ajoutez la variable *ITCAMDCHOME*. Définissez la valeur de la variable *ITCAMDCHOME* sur le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/agent/yndchome/7.3.0.14.06`.
13. Cliquez sur **Apply**, puis enregistrez les changements apportés à la configuration principale.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné dans les **options de préférence de la console**, puis cliquez sur **Sauvegarder**.
14. Redémarrez le serveur d'applications.

Résultats

Vous pouvez à présent vérifier les données de l'Agent WebSphere Applications dans la console Cloud APM après avoir ajouté ce composant d'application à vos applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour obtenir des instructions sur l'ajout ou l'édition d'une application, voir «Gestion des applications», à la page 1145.

Que faire ensuite

Après avoir configuré manuellement le collecteur de données, vous ne pouvez pas utiliser l'utilitaire `unconfig` fourni pour annuler la configuration du collecteur de données. Annulez plutôt la configuration du collecteur de données manuellement. Pour plus d'informations, voir «Annulation manuelle de la configuration du collecteur de données», à la page 195.

Configuration manuelle du collecteur de données pour WebSphere Application Server Liberty : Procédure

1. Accédez au répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Editez le fichier `jvm.options` en ajoutant les paramètres suivants, *base_cd* correspondant au répertoire de base du collecteur de données et *nom_serveur*, au nom du serveur Liberty. Si le fichier `jvm.options` n'existe pas, créez-le avec un éditeur de texte.

   ```
   -agentlib:am_ibm_16=nom_serveur
   –Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
   -verbosegc
   ```

   Lors de l'ajout de ces entrées, notez ce qui suit :

   - Chaque entrée doit se trouver sur une ligne distincte.
   - Remplacez *nom_serveur* par le nom réel du serveur Liberty. Par exemple, `defaultServer`.
   - Remplacez *base_cd* par le répertoire de base réel du collecteur de données. Par exemple, `/opt/ibm/apm/agent/yndchome/7.3.0.14.06`.
3. Ouvrez le fichier `server.env` dans le même répertoire et ajoutez le chemin suivant à l'entrée d'environnement en fonction du système d'exploitation, où *base_cd* correspond au répertoire de base du collecteur de données. Si le fichier `server.env` n'existe pas, créez-le avec un éditeur de texte.

Tableau 188. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/aix536`
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/aix536`
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:base_cd/toolkit/lib/lx8266`
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:base_cd/toolkit/lib/li6263`
Windows (machine virtuelle Java 32 bits)	PATH	`/lib;base_cd/toolkit/lib/win32`
Windows (machine virtuelle Java 64 bits)	PATH	`/lib;base_cd/toolkit/lib/win64`

4. Ouvrez le fichier `server.xml` dans le même répertoire et ajoutez les lignes suivantes pour activer la fonction de surveillance :

   ```
   <featureManager>
                <feature>webProfile-7.0</feature>
                <feature>monitor-1.0</feature>
                <feature>usr:itcam-730.140</feature>
      </featureManager>
   ```

5. Redémarrez le serveur Liberty.

Résultats

Vous pouvez à présent vérifier les données de l'Agent WebSphere Applications dans la console Cloud APM après avoir ajouté ce composant d'application à vos applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour obtenir des instructions sur l'ajout ou l'édition d'une application, voir «Gestion des applications», à la page 1145.

Que faire ensuite

Après avoir configuré manuellement le collecteur de données, vous ne pouvez pas utiliser l'utilitaire `unconfig` fourni pour annuler la configuration du collecteur de données. Annulez plutôt la configuration du collecteur de données manuellement. Pour plus d'informations, voir «Annulation manuelle de la configuration du collecteur de données», à la page 195.

(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données

Dans l'environnement de coexistence d'agent où l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications sont installés, vous devez effectuer certaines étapes de configuration supplémentaires pour l'agent et procéder différemment pour configurer le collecteur de données.

Pourquoi et quand exécuter cette tâche

Dans l'environnement de coexistence d'agent, vous ne configurez qu'un seul collecteur de données pour envoyer les données à l'Agent WebSphere Applications et à l'ITCAM Agent for WebSphere Applications. Les deux agents doivent utiliser des ports différents pour écouter les demandes du collecteur de données.

Procédure

1. Si le collecteur de données de l'ITCAM Agent for WebSphere Applications, installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring, est déjà présent dans votre environnement, désinstallez-le.
2. Installez l'Agent WebSphere Applications fourni dans IBM Cloud Application Performance Management 8.1.3 ou version ultérieure. Cela vous assure que la version 7.3.0.11.0 ou ultérieure du collecteur de données, qui est prise en charge pour la coexistence d'agent, est installée.
3. Assurez-vous que l'ID utilisateur employé pour configurer le collecteur de données et l'ID utilisateur employé pour installer le serveur d'applications disposent des droits d'utilisateur requis par l'agent. Pour plus d'informations, voir «Vérification des exigences d'accès utilisateur», à la page 769.
4. Assurez-vous que l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications utilisent des numéros de port différents pour écouter les demandes du collecteur de données. Les numéros de port doivent être uniques de façon à ne pas pouvoir être utilisés par aucun autre composant de votre environnement. Configurez à nouveau l'agent pour modifier le port, si nécessaire.
   - Pour plus d'informations sur la configuration de l'Agent WebSphere Applications, voir «Configuration de l'Agent WebSphere Applications», à la page 793.
   - Pour plus d'informations sur la configuration de l'ITCAM Agent for WebSphere Applications, consultez la documentation d'ITCAM for Application Diagnostics ou d'ITCAM for Applications.
5. Utilisez l'utilitaire de configuration fourni pour configurer le collecteur de données. Pour plus d'informations, voir «Configuration du collecteur de données pour l'environnement de coexistence d'agent», à la page 794.

   Conseil : Si vous maîtrisez la configuration du collecteur de données, vous pouvez également configurer le collecteur de données en mode silencieux. Pour plus d'informations, voir «Configuration du collecteur de données en mode silencieux», à la page 782.

Configuration de l'Agent WebSphere Applications :

Dans l'environnement de coexistence d'agent, le collecteur de données est partagé par l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications. Les deux agents doivent utiliser des ports différents pour écouter les demandes du collecteur de données. Vous devez configurer l'agent pour modifier le port, si nécessaire.

Pourquoi et quand exécuter cette tâche

- Sur les systèmes Linux ou AIX, vous pouvez configurer l'agent en mode interactif en exécutant le script de configuration, puis en répondant à des invites, ou en créant un fichier de réponses en mode silencieux et en exécutant le script de configuration sans interaction.
- Sur les systèmes Windows, vous pouvez configurer l'agent en créant le fichier de réponses silencieux et en exécutant le script de configuration, ou en lançant l'utilitaire Manage Monitoring Services. Pour plus d'informations sur Manage Monitoring Services sur des systèmes Windows, voir «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 217.

Procédure

- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :
  1. Créez un fichier `.txt` en tant que fichier de réponses silencieux.
  2. Indiquez les paramètres suivants dans le fichier de réponses silencieux. La syntaxe est *nom_paramètre=valeur_paramètre*.

     configure_type
     Indique le type de configuration. Ce paramètre est obligatoire.

     La valeur admise est `tema_configure` pour la configuration de l'agent.

     KYN_ALT_NODEID
     Indique l'ID de noeud alternatif pour identifier l'agent. Ce paramètre est obligatoire.

     La valeur admise est une chaîne alphanumérique pouvant inclure jusqu'à 24 caractères.

     KYN_PORT
     Indique le port d'écoute utilisé par l'agent. Il s'agit de la connexion socket TCP que l'agent utilise pour écouter les demandes de connexion du collecteur de données. Ce paramètre est obligatoire.

     La valeur par défaut est 63335.

     A faire : Dans un environnement de coexistence d'agent, vérifiez que le numéro de port indiqué n'est pas utilisé par l'ITCAM Agent for WebSphere Applications.

     Par exemple, ajoutez les lignes suivantes dans le fichier `.txt` que vous avez créé.

     ```
     configure_type=tema_configure
     KYN_ALT_NODEID=WASAgent
     KYN_PORT=63335
     ```

  3. Sauvegardez et fermez le fichier, puis entrez la commande suivante pour exécuter le script de configuration :
     - Linux AIX *rép_install*`/bin/was-agent.sh config` *chemin_fichier_réponses*
     - Windows *rép_install*`\bin\was-agent.bat config` *chemin_fichier_réponses*

     où *rép_install* est le répertoire d'installation de l'agent. La valeur par défaut est `C:\IBM\APM` sur les systèmes Windows et `/opt/ibm/apm/agent` sur les systèmes Linux et AIX.
  4. A l'issue de la configuration, redémarrez l'Agent WebSphere Applications s'il n'est pas encore en cours d'exécution à l'aide de la commande suivante :
     - Linux AIX *rép_install*`/bin/was-agent.sh start`

– Windows *rép_install*\bin\was-agent.bat start

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :
  1. A partir de la ligne de commande, accédez au répertoire *rép_install*/bin, où *rép_install* est le répertoire d'installation de l'agent.

     La valeur par défaut est /opt/ibm/apm/agent sur les systèmes Linux et AIX.
  2. Exécutez le script de configuration à partir du répertoire :

     ./was-agent.sh config
  3. A l'invite du système, entrez 1 et appuyez sur Entrée pour modifier les paramètres de l'Agent WebSphere Applications.
  4. Appuyez sur Entrée jusqu'à ce que le système vous invite à entrer l'ID de noeud alternatif pour identifier l'agent de surveillance.
  5. Indiquez l'ID noeud et appuyez sur Entrée. La valeur admise est une chaîne alphanumérique pouvant inclure jusqu'à 24 caractères.
  6. A l'invite du système, indiquez le port utilisé par l'agent pour écouter les demandes de connexion du collecteur de données et appuyez sur Entrée.

     A faire : Pour des environnements de coexistence d'agent, vérifiez que le port indiqué n'est pas utilisé par l'ITCAM Agent for WebSphere Applications.
  7. A l'issue de la configuration, redémarrez l'Agent WebSphere Applications.

Résultats

Vous avez configuré l'Agent WebSphere Applications.

Que faire ensuite

Vous devez ensuite configurer le collecteur de données. Lorsque vous configurez le collecteur de données, vous êtes invité à fournir le numéro de port que vous avez configuré pour l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications. Pour plus d'informations, voir «Configuration du collecteur de données pour l'environnement de coexistence d'agent».

Configuration du collecteur de données pour l'environnement de coexistence d'agent :

Si votre environnement inclut à la fois l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications, vous ne pouvez configurer qu'un seul collecteur de données pour les deux agents.

Avant de commencer

Assurez-vous que d'avoir terminé les autres étapes qui sont documentées dans «(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données», à la page 792.

Pourquoi et quand exécuter cette tâche

Exécutez l'utilitaire de configuration interactif fourni pour configurer le collecteur de données pour un environnement où l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications existent et partagent le collecteur de données.

Limitation : L'intégration du collecteur de données aux composants ou aux produits suivants n'est pas prise en charge pour l'ITCAM Agent for WebSphere Applications :

- ITCAM for Application Diagnostics Managing Server
- ITCAM for Transactions
- Tivoli Performance Viewer

A faire : La surveillance de WebSphere Application Server Liberty n'est pas prise en charge par l'ITCAM Agent for WebSphere Applications. Pour surveiller WebSphere Application Server Liberty, utilisez uniquement l'Agent WebSphere Applications. Pour plus d'informations sur la configuration du collecteur de données pour la surveillance Liberty, voir «Configuration du collecteur de données en mode interactif» , à la page 774 ou «Configuration du collecteur de données en mode silencieux», à la page 782.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. A partir de la ligne de commande, accédez au répertoire `bin` dans le répertoire *base_cd*. Le répertoire *base_cd* peut correspondre aux répertoires suivants :
   - Windows *rép_install*\dchome\7.3.0.14.06
   - Linux AIX *rép_install*/yndchome/7.3.0.14.06
3. Exécutez la commande suivante pour lancer l'utilitaire de configuration :
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   L'utilitaire de configuration démarre et affiche les adresses IP de toutes les cartes réseau détectées sur le système informatique local.
4. Entrez le nombre qui correspond à l'adresse IP à utiliser et appuyez sur Entrée. L'utilitaire de configuration affiche les répertoires de base de WebSphere Application Server qui ont été détectés sur le système.
5. Lorsque vous êtes invité à entrer le répertoire de base du serveur d'applications, entrez le numéro correspondant au répertoire de base de WebSphere Application Server ou un chemin d'accès complet au répertoire de base du serveur d'applications et appuyez sur Entrée.

   L'utilitaire de configuration affiche tous les profils de serveur d'applications détectés sous le répertoire de base indiqué.
6. Lorsque vous êtes invité à indiquer le profil du serveur d'applications à configurer, entrez le numéro correspondant au profil WebSphere Application Server et appuyez sur Entrée.

   L'utilitaire de configuration indique si la sécurité globale de WebSphere est activée pour le profil WebSphere Application Server que vous avez indiqué. Si la sécurité globale n'est pas activée, passez à l'étape 8.
7. Spécifiez si vous voulez récupérer les paramètres depuis un fichier de propriétés de client. Entrez `1` pour permettre à l'utilitaire de configuration d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié. Sinon, entrez `2` pour entrer le nom d'utilisateur et le mot de passe WebSphere.

   Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP. Si la sécurité globale est activée pour un profil de serveur d'applications, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à la console d'administration de WebSphere Application Server pour ce profil. Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI, ou le fichier `soap.client.props` pour une connexion SOAP.
8. Lorsque vous êtes invité à entrer le nom d'hôte de la console d'administration WebSphere, appuyez sur Entrée pour accepter les valeurs par défaut ou indiquez le nom d'hôte ou l'adresse IP de la console d'administration WebSphere. La valeur par défaut est `localhost`.
9. Lorsque l'utilitaire de configuration affiche une liste de toutes les instances de serveur qui ne sont pas encore configurées pour la collecte de données, sélectionnez une ou plusieurs instances de serveur d'applications dans la liste. Entrez le nombre qui correspond à l'instance de serveur d'applications à configurer pour la collecte de données ou entrez un astérisque (*) pour configurer

toutes les instances de serveur d'applications pour la collecte de données, puis appuyez sur Entrée. Pour spécifier un sous-ensemble de serveurs, entrez les numéros qui représentent les serveurs, séparés par des virgules. Par exemple, `1,2,3`.

A faire :

- Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration.
- Pour un environnement de déploiement réseau, Deployment Manager doit être en cours d'exécution.
- Assurez-vous que les instances de serveur d'applications que vous sélectionnez sont les serveurs réels qui hébergent les applications ou les services que vous voulez surveiller.

L'utilitaire de configuration fournit une option pour intégrer le collecteur de données pour l'Agent WebSphere Applications.

10. Dans la section **Integration with Agent for WebSphere Applications**, indiquez si vous souhaitez intégrer le collecteur de données à l'agent de surveillance. Vous devez entrer 1 pour sélectionner cette option d'intégration, puis appuyer sur Entrée. Le serveur sélectionné sera enregistré pour la surveillance des ressources PMI.
11. Indiquez si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications. Vous devez entrer 1 pour oui, puis appuyez sur Entrée.
12. Indiquez s'il faut activer ou non le collecteur de données pour les données de diagnostic. Entrez 1 pour oui ou 2 pour non.
13. Lorsque vous êtes invité à entrer le nom d'hôte de l'agent de surveillance V8, entrez le nom d'hôte ou l'adresse IP de l'Agent WebSphere Applications ou acceptez la valeur par défaut.
14. Lorsque vous êtes invité à entrer le numéro de port de l'agent de surveillance V8, entrez le numéro de port utilisé par l'Agent WebSphere Applications.

    A faire : La valeur par défaut peut ne pas être appropriée si elle est utilisée par un autre composant. Vous devez vous assurer que le port spécifié n'est pas utilisé par un autre composant dans votre environnement.
15. Indiquez si vous souhaitez configurer l'agent de surveillance V6. Entrez 1 pour configurer l'ITCAM Agent for WebSphere Applications et appuyez sur Entrée.
16. Lorsque vous êtes invité à entrer le nom d'hôte ou l'adresse IP de l'agent de surveillance V6, indiquez le nom d'hôte ou l'adresse IP de l'ITCAM Agent for WebSphere Applications.
17. Lorsque vous êtes invité à entrer le numéro de port de l'agent de surveillance V6, entrez le numéro de port utilisé par le composant agent de surveillance de l'ITCAM Agent for WebSphere Applications.

    A faire : La valeur par défaut peut ne pas être appropriée si elle est utilisée par un autre composant. Vous devez vous assurer que le port spécifié n'est pas utilisé par un autre composant dans votre environnement.
18. Lorsque vous êtes invité à entrer l'alias de serveur, n'utilisez pas la valeur par défaut et indiquez l'alias de serveur unique que vous souhaitez utiliser. Si vous configurez plusieurs instances de serveur d'applications, l'utilitaire de configuration vous invite à indiquer un alias pour chaque instance.

    Important : L'alias ne peut contenir que les caractères suivants : `A-Z`, `a-z`, soulignement (`_`), tiret (`-`) et point (`.`). N'utilisez pas d'autres caractères dans l'alias.

    L'alias de serveur est le premier qualificateur du nom d'instance d'agent (également appelé MSN) affiché sur la console Cloud APM. La valeur par défaut est le nom du noeud combiné au nom du serveur. Par exemple, l'alias **node1server1** indique le serveur **server1** dans le noeud **node1**.

19. Lorsque vous êtes invité à entrer le numéro de port TCP/IP pour la surveillance des ressources PMI, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un nouveau numéro. La valeur par défaut est `63355`.

    Le port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Si le port par défaut est déjà utilisé, définissez un numéro différent.
20. Dans la section **Prise en charge du suivi des transactions**, indiquez si vous souhaitez activer le suivi des transactions. Entrez `1` pour oui ou `2` pour non et passez à l'étape 22.

    A faire : Pour afficher les informations de suivi des transactions, vous devez activer le suivi des transactions dans la page Configuration d'agent de la console Cloud APM.
21. Acceptez le nom d'hôte ou l'adresse IP par défaut de Transaction Framework Extension, qui est un composant interne de l'Agent WebSphere Applications qui collecte les attributs depuis le collecteur de données.
22. Acceptez le numéro de port par défaut que le collecteur de données utilise pour se connecter à Transaction Framework Extension. La valeur par défaut est `5457`.
23. Indiquez si vous voulez intégrer le collecteur de données à Application Performance Diagnostics Lite. Appuyez sur Entrée pour accepter la valeur par défaut pour Non.
24. Dans la section **Paramètres avancés**, indiquez si vous souhaitez modifier le chemin du journal de la récupération de place. Entrez `1` pour sélectionner un chemin d'accès au journal de récupération de place. Autrement, entrez `2` et passez à l'étape 26.
25. Indiquez le chemin de la collecte de récupération de place. Entrez un nom de fichier avec son chemin d'accès complet.

    Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *`nom_profil`*`.`*`nom-cellule`*`.`*`nom_noeud`*`.`*`nom_serveur`*`.gc.log` pour chaque instance de serveur d'applications configurée.

    Important : Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que `%pid`.
26. Dans la section **Récapitulatif de la configuration du collecteur de données**, examinez le récapitulatif de la configuration du collecteur de données qui doit être appliquée aux instances de serveur d'applications indiquées. Si nécessaire, modifiez les paramètres de configuration.
27. Entrez `a` pour accepter les modifications.
28. A l'invite, indiquez si vous souhaitez créer une copie de sauvegarde de votre configuration en cours. Entrez `1` pour créer une sauvegarde de la configuration en cours. Sinon, entrez `2`.
29. Redémarrez les instances du serveur d'applications, comme indiqué par l'utilitaire de configuration.
    a. Accédez au répertoire `bin` situé sous le répertoire de base du profil de serveur d'applications. Par exemple, `opt/IBM/WebSphere/AppServer/profiles/`*`nom_profil`*`/bin`.
    b. Arrêtez le serveur d'applications en entrant la commande **`stopServer`** dans la console de commande.
       - Linux AIX `./stopServer.sh` *`nom_serveur`*
       - Windows `stopServer.bat` *`nom_serveur`*
    c. A l'invite, entrez l'ID utilisateur et le mot de passe de l'administrateur de la console d'administration WebSphere.
    d. Redémarrez le serveur d'applications en entrant la commande **`startServer`** dans la console de commande.
       - Linux AIX `./startServer.sh` *`nom_serveur`*
       - Windows `startServer.bat` *`nom_serveur`*

    La configuration du collecteur de données entre en vigueur une fois que le serveur d'applications a redémarré.

30. Connectez-vous à la console Cloud APM pour afficher les données dans les tableaux de bord.
    a. Ouvrez une fenêtre de navigateur et entrez l'adresse URL suivante, où *hôte_serveur* correspond à l'adresse IP du serveur :

       `https://hôte_serveur:9443`

    b. Lorsque vous êtes invité à indiquer votre ID de connexion, entrez les données d'identification suivantes pour l'utilisateur par défaut ou entrez les données d'identification qui ont été affectées à votre administrateur de console Cloud APM :
       - Nom d'utilisateur : *apmadmin*
       - Mot de passe : *apmpass*

       Les données d'identification utilisateur initiales après l'installation du serveur Cloud APM sont `apmadmin` avec le mot de passe `apmpass`.

    c. Utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillé au Tableau de bord d'Application Performance. Vous pouvez l'ajouter en tant que nouveau composant à votre application existante ou créer une application à laquelle ajouter ce composant. Pour plus d'informations sur l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

Que faire ensuite

- Si l'ID utilisateur actuel utilisé pour configurer le collecteur de données n'est pas identique à l'ID de l'utilisateur qui exécute le serveur d'applications, vérifiez que l'ID utilisateur de configuration du collecteur de données dispose des droits en lecture et en écriture sur les répertoires `runtime` et `logs` dans le répertoire de base du collecteur de données. Ces deux sous-répertoires sont créés par l'ID de l'utilisateur qui exécute le serveur d'applications lorsque le serveur est redémarré.
- Pour l'Agent WebSphere Applications, connectez-vous à la console Cloud APM pour afficher les données de surveillance dans les tableaux de bord. Pour l'ITCAM Agent for WebSphere Applications, connectez-vous à Tivoli Enterprise Portal pour afficher les données. Si les données de surveillance ne sont pas disponibles immédiatement, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
  - Windows

    ```
    cd rép_install\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

    ```
    cd rép_install/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

- La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si ce n'est pas la première fois que vous configurez le collecteur de données et que vous avez modifié l'alias de serveur, vous devez vider certains fichiers cache en effectuant les opérations suivantes :
  1. Arrêtez l'agent de surveillance s'il est en cours d'exécution.
  2. Ouvrez le fichier *nom_hôte*`_yn.xml` dans le répertoire suivant avec un éditeur de texte, où *nom_hôte* est le nom de l'hôte où l'Agent WebSphere Applications ou l'ITCAM Agent for WebSphere Applications est installé.
     - Windows *rép_install*`\TMAITM6_x64` (la valeur par défaut est `C:\IBM\APM\TMAITM6_x64` pour l'Agent WebSphere Applications ou `C:\IBM\ITM\TMAITM6_x64` pour l'ITCAM Agent for WebSphere Applications)
     - Linux AIX *rép_install*`/config` (La valeur par défaut est `/opt/ibm/apm/agent/config` pour l'Agent WebSphere Applications ou `/opt/ibm/itm/agent/config` pour l'ITCAM Agent for WebSphere Applications)

3. Recherchez la ligne qui commence par la chaîne suivante et qui contient le nom de serveur précédent. Par exemple `was85.win4net01Cell02.win4net01Node02.AppSrv01.server1`, où `server1` est le nom précédent du serveur d'applications.

   ```
   <!ENTITY code_produit_was.nom_cellule.nom_noeud.nom_profil.nom_serveur
   ```

   où *code_produit_was* est le code produit de WebSphere Application Server ; *nom_cellule* est le nom de la cellule ; *nom_noeud* est le nom du noeud ; *nom_profil* est le nom du profil de serveur d'applications ; *nom_serveur* est le nom précédent du serveur d'applications.
4. Dans le répertoire en cours, recherchez le fichier .XML indiqué sur la ligne et supprimez-le.
5. Supprimez la ligne que vous avez recherchée à l'étape 3 dans le fichier *nomhôte*`_yn.xml`.
6. A la fin du fichier *nom_hôte*`_yn.xml`, supprimez la ligne qui contient les noms de serveur précédents.
7. Sauvegardez et fermez le fichier.
8. Redémarrez l'agent de surveillance.

Reconfiguration du collecteur de données en cas de modification du type d'offre sur le serveur Cloud APM

Si vous avez modifié le type d'offre que vous avez installé sur le serveur Cloud APM (de Cloud APM, Base à Cloud APM, Advanced) et que l'Agent WebSphere Applications a été installé et configuré avec l'offre Cloud APM, Base, vous devez, pour pouvoir utiliser les fonctions avancées de l'agent fournies dans l'offre Cloud APM, Advanced, désinstaller l'Agent WebSphere Applications précédent et réinstaller l'agent avec l'offre Cloud APM, Advanced. Vous pouvez aussi reconfigurer le collecteur de données pour que les fonctionnalités soient disponibles dans la nouvelle offre.

Pourquoi et quand exécuter cette tâche

La configuration de l'Agent WebSphere Applications est différente selon le package d'agent utilisé pour installer l'agent. Après avoir modifié le type d'offre sur le serveur Cloud APM, vous disposez de deux options pour activer les fonctionnalités d'agent de la nouvelle offre :

- Supprimez l'agent que vous avez installé avec l'offre précédente, puis installez l'agent de la nouvelle offre.
- Reconfigurez le collecteur de données pour utiliser les fonctionnalités de la nouvelle offre.

Procédure

- Supprimez l'agent que vous avez installé avec l'offre précédente, puis installez l'agent de la nouvelle offre.
  1. Annulez la configuration du collecteur de données. Pour plus d'informations, voir «Agent WebSphere Applications : Annulation de la configuration du collecteur de données», à la page 189.
  2. Désinstallez l'Agent WebSphere Applications que vous avez installé avec le package d'agent de l'offre précédente. Pour plus d'informations, voir «Désinstallation de vos agents», à la page 187.
  3. Installez l'Agent WebSphere Applications avec le package d'agent de la nouvelle offre, puis reconfigurez le collecteur de données. Pour plus d'informations, voir «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 771.
- Reconfigurez le collecteur de données pour utiliser les fonctionnalités de la nouvelle offre.
  1. Editez le fichier `offering.id` dans le répertoire de base du collecteur de données en remplaçant la valeur **`IOFFERING`** par l'une des valeurs suivantes, selon le nouveau type d'offre :

     BASE Si votre nouveau type d'offre est Cloud APM, Base Private.

     ADVANCED
     Si votre nouveau type d'offre est Cloud APM, Advanced Private.

     Le répertoire de base du collecteur de données est le suivant :

     – Windows *rép_install*`\dchome\7.3.0.14.06`

– Linux AIX *rép_install*/yndchome/7.3.0.14.06

2. Reconfigurez le collecteur de données pour activer les fonctions de diagnostic, de suivi des transactions ou les deux dans le collecteur de données, sur la base des fonctionnalités prises en charge dans le nouveau type d'offre. Pour savoir comment configurer le collecteur de données, voir «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 771.
3. Redémarrez WebSphere Application Server.
4. Dans une page de la console Cloud APM, cliquez sur **Configuration du système** > **Configuration d'agent** pour ouvrir la page Configuration d'agent. Assurez-vous que le paramètre de suivi des transactions correspond aux fonctionnalités disponibles dans votre nouveau type d'offre. Sinon, mettez le paramètre à jour.

   Le paramètre de suivi des transactions doit être activé pour Cloud APM, Advanced, mais désactivé pour Cloud APM, Base.

Surveillance de WebSphere Application Server Liberty dans un conteneur Docker

Pour surveiller un profil Liberty dans un conteneur Docker, vous devez utiliser la commande **docker run** avec quelques options afin de configurer le collecteur de données pour que WebSphere Application Server Liberty puisse démarrer.

Avant de commencer

Vous devez installer Agent WebSphere Applications sur l'hôte Docker.

Pourquoi et quand exécuter cette tâche

Chaque profil Liberty qui s'exécute dans un conteneur Docker nécessite un collecteur de données pour collecter des mesures de ressource, des mesures de transaction et des données de diagnostic, puis transmettre les données à l'agent de surveillance qui s'exécute sur l'hôte Docker. Tous les collecteurs de données configurés sur le même hôte Docker se partagent le même agent de surveillance sur l'hôte.

Procédure

Pour configurer le collecteur de données pour un conteneur de profil Liberty, procédez comme suit :

1. Créez un fichier de réponses silencieux `.txt`, indiquez les options de configuration suivantes dans le fichier et enregistrez-le.

   ```
   tema.host=hôte_agent
   was.appserver.server.name=nom_profil_liberty
   ```

   où **tema.host** permet d'indiquer l'adresse IP de l'hôte de l'agent de surveillance et **was.appserver.server.name** le nom du profil Liberty.

   Conseil : Un exemple de fichier de réponses silencieux (`sample_silent_liberty_config.txt`) est fourni dans le répertoire *<rép_install_agent>*`/agent/yndchome/7.3.0.14.06/bin`. Vous pouvez créer votre propre fichier de réponses en vous basant sur cet exemple.
2. Exécutez la commande suivante pour démarrer le nouveau conteneur Docker. Vous devez accepter la licence pour finaliser la configuration en définissant le paramètre **LICENSE** sur `accept`.

   ```
   $docker run -d -e LICENSE=accept \
   -e JAVA_HOME=<rép_base_java> \
   -p <numéro_port>:<numéro_port> \
   -v <rép_app_web>:<rép_install_liberty>/usr/servers/<nom_profil_liberty> \
   -v <rép_install_agent>/agent/yndchome:<rép_install_agent>/agent/yndchome
   websphere-liberty /bin/bash \
   -c "<rép_install_agent>/agent/yndchome/<version_cd>/bin/config.sh -silent
   <absolute_path_to_silent_response_file> && <rép_install_liberty>/bin/server
   run <nom_profil_liberty>"
   ```

   Où :

- <*rép_base_java*> est le répertoire de l'environnement d'exécution Java qu'utilise le profil Liberty. Par exemple, `/opt/ibm/java/jre`.
- <*numéro_port*> est le numéro du port utilisé pour la communication entre le conteneur et l'hôte.
- <*rép_app_web*> est le répertoire dans lequel se trouve l'application Web.
- <*rép_install_liberty*> est le répertoire d'installation de WebSphere Application Server Liberty. Par défaut, il s'agit du répertoire `/opt/ibm/wlp`.
- <*nom_profil_liberty*> est le nom du profil Liberty.
- <*rép_install_agent*> est le répertoire d'installation de l'Agent WebSphere Applications. Par défaut, il s'agit du répertoire `/opt/ibm/apm`.
- <*version_cd*> est le numéro de version du collecteur de données pour l'Agent WebSphere Applications. Par exemple, 7.3.0.14.06.
- <*chemin_absolu_fichier_réponses_silencieux*> est le chemin d'accès absolu au fichier de réponses silencieux que vous avez créé.

Par exemple, la commande suivante configure le collecteur de données pour le profil Liberty nommé newitcam. L'Agent WebSphere Applications et le profil Liberty sont tous deux installés dans les répertoires par défaut. La version de l'agent de surveillance et du collecteur de données est 7.3.0.14.06.

```
$docker run -d -e LICENSE=accept \
-e JAVA_HOME=/opt/ibm/java/jre \
-p 9082:9082 \
-v /home/kub/liberty-docker/newitcam:/opt/ibm/wlp/usr/servers/newitcam \
-v /opt/ibm/apm/agent/yndchome:/opt/ibm/apm/agent/yndchome websphere-liberty
/bin/bash \
-c "/opt/ibm/apm/agent/yndchome/7.3.0.14.06/bin/config.sh -silent
/opt/ibm/wlp/usr/servers/newitcam/silent_config.txt && /opt/ibm/wlp/bin/server
run newitcam"
```

Résultats

Vous pouvez à présent vérifier que les données de l'Agent WebSphere Applications s'affichent dans la console Cloud APM. La colonne **Nom de la cellule** du widget **Informations WAS** affiche l'ID du conteneur Docker où s'exécute le profil Liberty.

Que faire ensuite

Pour annuler la configuration du collecteur de données de manière interactive, utilisez la commande suivante pour démarrer l'utilitaire d'annulation de configuration :

```
docker exec -i id_conteneur "<rép_install_agent>/yndchome/7.3.0.14.06/bin
/unconfig.sh"
```

Configuration manuelle du collecteur de données en vue de surveiller des serveurs de cluster dynamique

Vous pouvez configurer le collecteur de données pour surveiller des instances de serveur d'applications dans un cluster dynamique en ajoutant quelques paramètres de configuration de collecteur de données au modèle de serveur utilisé pour créer les instances de serveur de cluster dynamique. C'est une méthode alternative à la création de modèles de serveur spécifiques pour l'Agent WebSphere Applications pour configurer des instances de serveur de cluster dynamique.

Pourquoi et quand exécuter cette tâche

Pour configurer le collecteur de données pour la surveillance des clusters dynamiques, vous devez créer deux fichiers de paramètres, puis ajouter manuellement les paramètres dans la console d'administration WebSphere afin de modifier le modèle de serveur dynamique. Le répertoire `d'exécution` est créé automatiquement lorsque le collecteur de données est démarré pour l'instance de serveur d'applications. Toute mise à niveau du modèle de serveur supprime les modifications effectuées de cette manière.

Important :

- Le nom de cluster ne doit pas contenir d'espace.
- Vous devez apporter des modifications manuelles à la configuration WebSphere Application Server pour les collecteurs de données en tant qu'administrateur WebSphere.
- Vous devez être un administrateur WebSphere expérimenté pour apporter des modifications manuelles à WebSphere Application Server en vue de la collecte de données. Toute erreur dans la modification manuelle de la configuration peut empêcher le démarrage du serveur d'applications.
- Si vous configurez manuellement le collecteur de données pour surveiller des instances de serveur d'application, vous ne pouvez pas employer l'utilitaire d'annulation de configuration pour annuler la configuration du collecteur de données. Pour annuler la configuration du collecteur de données, vous devez rétablir manuellement les paramètres.

Procédure

1. Créez le fichier `dcManualInput.txt` dans le répertoire `runtime` du collecteur de données. Suivez les instructions décrites dans «Création du fichier `dcManualInput.txt`».
2. Créez le fichier `itcam_wsBundleMetaData.xml` dans le répertoire `wsBundleMetaData` du collecteur de données. Suivez les instructions décrites dans «Création du fichier `itcam_wsBundleMetaData.xml`», à la page 804.
3. Utilisez la console d'administration WebSphere pour modifier le modèle de serveur dynamique en ajoutant le paramètre de configuration du collecteur de données. Suivez les instructions décrites dans «Ajout de paramètres avec la console d'administration WebSphere», à la page 805.

   Conseil : Le nom de membre du cluster dynamique est utilisé comme qualificateur du milieu dans le nom d'instance de l'Agent WebSphere Applications affiché dans la console Cloud APM. Il est possible que le nom de membre du cluster soit tronqué en raison du nombre maximal de caractères dans le nom d'instance de l'agent. Dans ce cas, vous pouvez modifier le modèle du serveur dynamique en ajoutant une variable nommée *${MEP_NAME}* et en lui attribuant le nom de machine virtuelle Java pour chaque instance de serveur. Vous pouvez ensuite distinguer chaque membre du cluster à l'aide du nom de machine virtuelle Java réel dans la console Cloud APM. Pour plus d'informations, voir «Facultatif : Affichage du nom de machine virtuelle réel pour établir une distinction entre les membres du cluster», à la page 807.

Création du fichier `dcManualInput.txt` : Pourquoi et quand exécuter cette tâche

Le fichier `dcManualInput.txt` contient certaines valeurs obligatoires pour la configuration initiale du collecteur de données.

Procédure

Pour créer le fichier `dcManualInput.txt`, procédez comme suit :

1. Vérifiez s'il existe un fichier nommé *plateforme*`_Template.DCManualInput.txt` dans le répertoire suivant. S'il n'existe pas, créez-le.
   - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/runtime`
   - Windows *rép_install*`\dchome\7.3.0.14.06\runtime`

   La variable *plateforme* dans le nom du fichier désigne l'architecture du système d'exploitation, par exemple, aix32, xLinux64.

   Vous pouvez attribuer au fichier le nom qui vous convient. Toutefois, *plateforme*`_Template.DCManualInput.txt` respecte les conventions d'attribution de nom lorsque le fichier est créé en exécutant le script `configtemplate.sh`. Vous devrez indiquer ce fichier pour le modèle de serveur avec la console d'administration WebSphere à la prochaine étape.
2. Copiez le contenu du fichier suivant dans le fichier `.txt` que vous avez trouvé ou créé à l'étape précédente.

- Linux AIX *base_cd*/itcamdc/etc/was/dcInput_manual.properties
- Windows *base_cd*\itcamdc\etc\was\dcInput_manual.properties

3. Editez le contenu du fichier .txt. Vous devez définir les paramètres de la section 1 du fichier en fonction des descriptions fournies dans tableau 189.

A faire :

- Ne modifiez pas les paramètres de la section 2.
- Certains des paramètres de configuration qu'utilise le collecteur de données pour créer les répertoires d'exécution sont toujours définis sur none. En effet, dans la surveillance des clusters dynamiques, le collecteur de données utilise la configuration de l'instance de serveur WebSphere pour créer les répertoires au démarrage de la machine virtuelle Java.

Tableau 189. Paramètres de configuration de la section 1

Paramètre	Valeur
local.hostname	Adresse IP ou nom de domaine qualifié complet du système local.
was.profile.home	Répertoire de base du profil. Toujours définir sur none pour un serveur de cluster dynamique
was.version	Numéro de version abrégé. Toujours définir sur none pour un serveur de cluster dynamique
itcam.home	Répertoire de base du collecteur de données. Exemple : /opt/ibm/apm/agent/yndchome/7.3.0.14.06
was.nodename	Nom du noeud. Toujours définir sur none pour un serveur de cluster dynamique
was.servername	Nom du serveur. Toujours définir sur none pour un serveur de cluster dynamique
was.profilename	Nom du profil WebSphere. Toujours définir sur none pour un serveur de cluster dynamique
am.camtoolkit.gpe.dc.operation.mode	Mode de fonctionnement du collecteur de données. Les valeurs admises sont toute combinaison de WR, TT et DE, où : **WR** Intègre le collecteur de données à l'Agent WebSphere Applications. **TT** Intègre le collecteur de données à ITCAM for Transactions. **DE** Intègre le collecteur de données à l'outil de diagnostics d'ITCAM. L'outil est présent dans la version bêta d'ITCAM for Application Diagnostics. Vous ne devez indiquer que les modes de fonctionnement obligatoires. Par exemple, si vous connectez le collecteur de données uniquement à l'Agent WebSphere Applications, indiquez WR. Séparez les modes de fonctionnement avec une virgule. Exemple : am.camtoolkit.gpe.dc.operation.mode=WR, DE
interp	Code de plateforme. Exemple : interp=win64 ou interp=lx6266

Tableau 189. Paramètres de configuration de la section 1 (suite)

Paramètre	Valeur
kwj.serveralias	Nom d'alias de WebSphere Application Server. Toujours définir sur `none` pour un serveur de cluster dynamique
temagclog.path	(Facultatif) Nom du chemin d'accès au fichier journal de récupération de place. Entrez un nom de fichier unique avec son chemin complet. Le nom de chemin ne doit pas contenir d'espaces.
tema.host	Nom d'hôte ou adresse IP de l'Agent WebSphere Applications. Obligatoire si le mode de fonctionnement inclut l'Agent WebSphere Applications (`WR`). En général, l'agent de surveillance est installé sur chaque système où le collecteur de données s'exécute et l'adresse de bouclage peut être indiquée. Exemple : `tema.host=127.0.0.1`
tema.port	Port à utiliser pour communiquer avec l'Agent WebSphere Applications. Obligatoire si le mode de fonctionnement inclut l'Agent WebSphere Applications (`WR`). La valeur par défaut est 63335. Exemple : `tema.port=63335`
tt.connection.string	Nom d'hôte ou adresse IP et numéro de port du composant collecteur de transaction d'ITCAM for Transactions au format `tcp:`*`nom_hôte`*`(IP):`*`port`*. Obligatoire si le mode de fonctionnement inclut ITCAM for Transactions (`TT`). Exemple : `tt.connection.string=192.38.234.77:5455`

4. Ajoutez les lignes suivantes à la section 1 du fichier `.txt`.

```
bcm.helper=com.ibm.tivoli.itcam.was.bcm.websphere.DefaultWASBCMHelper
BCM_HELPER=@{bcm.helper}
```

5. Sauvegardez et fermez le fichier.

Création du fichier `itcam_wsBundleMetaData.xml` :
Pourquoi et quand exécuter cette tâche

Le fichier `itcam_wsBundleMetaData.xml` contient certaines des valeurs obligatoires pour la configuration initiale du collecteur de données.

Procédure

Pour créer ce fichier, procédez comme suit :

1. Créez un répertoire nommé `wsBundleMetaData` dans le répertoire suivant :
   - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/runtime`
   - Windows *rép_install*`\dchome\7.3.0.14.06\runtime`
2. Créez un fichier nommé `itcam_wsBundleMetaData.xml` et copiez dans ce fichier le contenu du fichier suivant :
   - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/itcamdc/etc/was/itcam_wsBundleMetaData_template.xml`
   - Windows *rép_install*`\dchome\7.3.0.14.06\itcamdc\etc\was\itcam_wsBundleMetaData_template.xml`
3. Dans le fichier `itcam_wsBundleMetaData.xml`, remplacez la variable *@{CONFIGHOME}* par le chemin d'accès complet au répertoire de base de votre collecteur de données. Sur chaque système d'exploitation, le répertoire de base du collecteur de données est le suivant :

- Linux AIX *rép_install*/yndchome/7.3.0.14.06
- Windows *rép_install*\dchome\7.3.0.14.06

4. Placez le fichier itcam_wsBundleMetaData.xml dans le répertoire wsBundleMetaData créé à l'étape 1.

Ajout de paramètres avec la console d'administration WebSphere : Procédure

Pour modifier le modèle de serveur dynamique avec la console d'administration WebSphere, procédez comme suit :

1. Connectez-vous à la console d'administration WebSphere.
2. Cliquez sur **Serveurs**.
3. Développez **Clusters**, puis sélectionnez **Clusters dynamiques**.
4. Cliquez sur le nom du cluster de serveurs dynamiques à configurer avec le collecteur de données.
5. Dans la section **Propriétés supplémentaires**, cliquez sur **Modèle de serveur**.
6. Dans la section **Infrastructure du serveur**, développez **Gestion des processus et Java**, puis cliquez sur **Définition des processus**.
7. Dans la section **Propriétés supplémentaires**, cliquez sur **Machine virtuelle Java**.
8. Dans la zone **Arguments JVM génériques**, ajoutez les entrées suivantes :

   ```
   -agentlib:am_$jvm-vendor_$jvm-version=${WAS_SERVER_NAME}
   -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
   -verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
   $platform_Template_DCManualInput.txt
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000
   -Dsun.rmi.transport.connectionTimeout=300000
   -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
   –Ditcamdc.dyncluster=true
   ```

   Lors de l'ajout de ces entrées, notez les éléments suivants :
   - Toutes les entrées doivent se trouver sur une seule ligne.
   - Séparez les différents arguments par des espaces avant le signe -. N'utilisez pas d'espaces ailleurs.
   - Remplacez les variables suivantes par les noms réels :
     - *$jvm-vendor* : fournisseur de machine virtuelle Java utilisé.
     - *$jvm-version* : informations sur la version de machine virtuelle Java, telles que base 15 sur Java 5, base 16 sur Java 6 ou base 17 sur Java 7.
     - *$platform_Template_DCManualInput.txt* : fichier .txt créé à l'étape précédente.

   Exemple :

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME}
   -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
   -verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
   aix64_Template_DCManualInput.txt
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000
   -Dsun.rmi.transport.connectionTimeout=300000
   -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
   –Ditcamdc.dyncluster=true
   ```

9. Cliquez sur **Appliquer**.
10. Dans la boîte de dialogue Messages, cliquez sur **Sauvegarder**.
11. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.

- Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.

12. Revenez dans **Clusters**, cliquez sur **Clusters dynamiques**, puis sur le même nom de serveur.
13. Dans l'onglet **Configuration**, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
14. Selon le système d'exploitation, la plateforme matérielle et la machine virtuelle Java de serveur d'applications utilisés, définissez l'entrée d'environnement suivante :

Tableau 190. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
AIX R7.1 (machine virtuelle Java 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx8266:${ITCAMDCHOME}/toolkit/lib/lx8266/ttapi
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx6263:${ITCAMDCHOME}/toolkit/lib/lx6263/ttapi
Linux ppc R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp263:${ITCAMDCHOME}/toolkit/lib/lpp263/ttapi
Linux ppc R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp266:${ITCAMDCHOME}/toolkit/lib/lpp266/ttapi
Windows (machine virtuelle Java 32 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win32;${ITCAMDCHOME}/toolkit/lib/win32/ttapi
Windows (machine virtuelle Java 64 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win64;${ITCAMDCHOME}/toolkit/lib/win64/ttapi

15. Définissez le nom d'entrée d'environnement NLSPATH sur la valeur suivante :
    ${ITCAMDCHOME}/toolkit/msg/%L/%N.cat
16. Cliquez sur **Appliquer**, puis sur **Sauvegarder**.
17. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
18. Revenez dans **Clusters**, cliquez sur **Clusters dynamiques**, puis sur le même nom de serveur.
19. Dans l'onglet **Configuration**, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java** > **Propriétés supplémentaires : Propriétés personnalisées**.

20. Cliquez sur **Nouveau** pour ajouter les paires nom-valeur suivantes, puis cliquez sur **Appliquer**.
    - Créez une propriété `am.home` et définissez sa valeur sur le répertoire suivant :
      - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/itcamdc`
      - Windows *rép_install*`\dchome\7.3.0.14.06\itcamdc`
    - Créez une propriété `am.orig.wascell` et définissez sa valeur sur le répertoire de cellule. Par exemple, `am.orig.wascell =cellname1`.
    - Créez une propriété `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild` et définissez sa valeur sur `true`.
    - Créez une propriété `ITCAM_DC_ENABLED` et définissez sa valeur sur `true`.
    - Créez une propriété `TEMAGCCollector.gclog.path`. Si l'argument `verlogsegclog` de la machine virtuelle Java générique est défini, définissez la propriété `TEMAGCCollector.gclog.path` sur la même valeur. Sinon, définissez la propriété `TEMAGCCollector.gclog.path` sur `None`.

      Conseil : Pour identifier la valeur de la propriété `verlogsegclog`, dans l'onglet **Configuration**, cliquez sur **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java**. La valeur de `verlogsegclog` est indiquée dans la zone **Arguments JVM génériques**.
21. Dans la boîte de dialogue Messages, cliquez sur **Sauvegarder**.
22. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné. Cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
23. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
24. Définissez les variables suivantes. Pour chaque variable, vous devez choisir le niveau de portée approprié, en fonction du répertoire d'installation du collecteur de données sur les divers systèmes. Si les systèmes ont différents répertoires d'installation pour le collecteur de données, ces variables doivent être correctement définies pour chaque portée de niveau noeud. S'ils ont tous le même répertoire d'installation, la portée peut être plus élevée, par exemple au niveau cluster.
    - Définissez *ITCAMDCHOME* sur le répertoire suivant :
      - Linux AIX *rép_install*`/yndchome/7.3.0.14.06/itcamdc`
      - Windows *rép_install*`\dchome\7.3.0.14.06\itcamdc`
    - Définissez *ITCAMDCVERSION* sur la version du collecteur de données, par exemple, 7.3.0.14.06.
25. Cliquez sur **Appliquer**, puis sur **Sauvegarder**.
26. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.

    Une fois le modèle modifié, les valeurs sont synchronisées avec toutes les instances de serveur du cluster dynamique. Tout nouveau serveur créé de manière dynamique aura les mêmes paramètres de configuration de collecteur de données.
27. Redémarrez l'instance de serveur d'applications pour le collecteur de données à activer. Le collecteur de données lit les fichiers de paramètres et crée le répertoire d'exécution.

Facultatif : Affichage du nom de machine virtuelle réel pour établir une distinction entre les membres du cluster :

Pourquoi et quand exécuter cette tâche

Sur la console Cloud APM, le nom d'instance de l'Agent WebSphere Applications prend la forme *nom_hôte*::*nom_serveur_was*:KYNS et contient 32 caractères au maximum. Dans un environnement de cluster dynamique, les noms de membre du cluster dynamique sont utilisés comme qualificateurs du milieu *nom_serveur_was*.

Il est possible que les noms de membre du cluster soient tronqués en raison du nombre maximal de caractères. Dans ce cas, vous pouvez indiquer le nom de machine virtuelle Java réel à utiliser comme qualificateur du milieu dans le nom d'instance d'agent.

Procédure

Pour afficher le nom de machine virtuelle réel dans le nom d'instance de l'agent, procédez comme suit :

1. Connectez-vous à la console d'administration WebSphere pour mettre à jour les arguments génériques de machine virtuelle Java en ajoutant une nouvelle variable d'environnement *${MEP_NAME}* de la manière suivante :

   ```
   -agentlib:am_$jvm-vendor_$jvm-version=${MEP_NAME}${WAS_SERVER_NAME}
   -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
   -verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
   $platform_Template_DCManualInput.txt
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000
   -Dsun.rmi.transport.connectionTimeout=300000
   -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
   –Ditcamdc.dyncluster=true
   ```

   Exemple :

   ```
   -agentlib:am_ibm_16=${MEP_NAME}${WAS_SERVER_NAME}
   -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
   -verbosegc
   -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
   aix64_Template_DCManualInput.txt
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000
   -Dsun.rmi.transport.connectionTimeout=300000
   -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
   –Ditcamdc.dyncluster=true
   ```

2. Sauvegardez et appliquez les modifications.
3. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere** pour définir la variable *${MEP_NAME}* pour chaque membre du cluster dynamique. Définissez la valeur en indiquant le nom réel de machine virtuelle réel du membre du cluster.
4. Sauvegardez et appliquez les modifications.
5. Redémarrez l'instance du serveur d'applications.

   La console Cloud APM affiche une nouvelle instance de l'Agent WebSphere Applications dont le nom contient la valeur *${MEP_NAME}* que vous venez d'indiquer.

Configuration dynamique de la collecte des données sur la page Configuration d'agent

Une fois que vous avez activé la prise en charge du suivi des transactions ou de la collecte des données de diagnostic dans le collecteur de données, utilisez la page Configuration d'agent pour activer ou désactiver la collecte des données de manière dynamique.

Avant de commencer

- Vous devez installer et configurer l'Monitoring Agent for WebSphere Applications.

- Pour activer ou désactiver le suivi des transactions pour les serveurs d'applications surveillés, vous devez installer Suivi des transactions. Vous devez également activer la prise en charge du suivi des transactions sur l'agent, comme décrit dans «Configuration du collecteur de données en mode interactif», à la page 774. Si vous suivez la procédure de configuration simple, le collecteur de données est automatiquement configuré avec la prise en charge du suivi des transactions.
- Pour activer ou désactiver la collecte des données de diagnostic et notamment la trace de méthode, vous devez posséder Cloud APM, Advanced Private. Vous devez également activer la prise en charge de la collecte des données de diagnostic et des informations de trace de méthode dans le collecteur de données, comme décrit dans «Configuration du collecteur de données en mode interactif», à la page 774. (Non disponible pour Cloud APM, Base Private).

Conseil : La page Configuration de l'agent affiche tous les serveurs surveillés par l'agent. Si un serveur manque, il risque de ne pas être correctement surveillé. Recherchez les messages d'erreur, par exemple de connexion, dans les fichiers journaux d'agent sur le système surveillé.

A faire : L'Agent WebSphere Applications ne prend en charge que Db2 et Oracle comme source de données. Pour les autres types de source de données, certaines valeurs d'indicateur clé de performance pourraient apparaître comme nulles dans les tableaux de bord de suivi des transactions et les widgets de groupe.

Procédure

Pour configurer la collecte des données pour chaque serveur, procédez comme suit :

1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
2. Cliquez sur l'onglet **WebSphere Applications**.
3. Cochez les cases des serveurs sur lesquels vous voulez configurer la collecte de données et effectuez l'une des actions suivantes de la liste **Actions** :
   - Pour activer le suivi des transactions, cliquez sur **Activer le suivi des transactions**. Le statut dans la colonne **Suivi des transactions en cours** est mis à jour et indique Oui pour chaque serveur sélectionné.
   - Pour activer uniquement la collecte des données de diagnostic, cliquez sur **Activer le mode diagnostic**. Le statut dans la colonne **Mode diagnostic en cours** est mis à jour et indique Oui pour chaque serveur sélectionné.
   - Pour collecter à la fois les données de diagnostic et les informations de trace de méthode, cliquez sur **Activer le mode diagnostic et la trace de méthode**. Le statut dans les colonnes **Mode diagnostic en cours** et **Trace de méthode en cours** est mis à jour et indique Oui pour chaque serveur sélectionné.
   - Pour désactiver le suivi des transactions pour le serveur sélectionné, cliquez sur **Désactiver le suivi des transactions**. Le statut dans la colonne **Suivi des transactions en cours** est mis à jour et indique Non pour chaque serveur sélectionné.
   - Si seule la collecte des données de diagnostic est activée pour le serveur sélectionné, pour désactiver la collecte des données, cliquez sur **Désactiver le mode diagnostic**. Le statut dans la colonne **Mode diagnostic en cours** est mis à jour et indique Non pour chaque serveur sélectionné.
   - Si les données de diagnostic et les données de trace de méthode sont activées pour le serveur sélectionné, pour désactiver la collecte des données, cliquez sur **Désactiver le mode diagnostic et la trace de méthode**. Le statut dans les colonnes **Mode diagnostic en cours** et **Trace de méthode en cours** est mis à jour et indique Non pour chaque serveur sélectionné.

   A faire :
   - A moins que le support du suivi des transactions ou de la collecte des données de diagnostic soit configuré dans le collecteur de données, les opérations sur la page Configuration d'agent n'activent pas la collecte des données et la valeur de la colonne est définie sur Non.

- Si le profil du serveur d'applications a été configuré pour utiliser `127.0.0.1` comme nom d'hôte, la colonne **Adresse IP** de la page Configuration d'agent affiche l'adresse IP de l'hôte où l'Agent WebSphere Applications est installé et en cours d'exécution.

Résultats

Vous avez configuré la collecte des données pour chaque serveur sélectionné. Les données de suivi des transactions et de diagnostic peuvent être affichées dans les tableaux de bord de topologie une fois que vous avez activé la collecte de données.

Important : Si un serveur d'application redémarre, il se peut que vous deviez réactiver le suivi des transactions ou la collecte des données de diagnostic pour le serveur.

Activation de la surveillance des fuites de mémoire

Pour que le tableau de bord Analyse de mémoire contienne des données, vous devez activer la surveillance des fuites de mémoire pour le collecteur de données. Si le JRE qui est utilisé par le serveur d'applications est pris en charge, la fonction de surveillance des fuites de mémoire est activée par défaut une fois que vous avez activé la collecte de données de diagnostic.

Avant de commencer

- Assurez-vous que `-Xtrace:none` n'est pas défini dans les arguments JVM pour le serveur d'applications.
- Lorsque la fonction de surveillance des fuites de mémoire est activée, les paramètres suivants sont définis dans les arguments JVM pour le serveur d'applications. Si vous avez défini ces paramètres dans vos arguments JVM en cours, assurez-vous que la configuration du collecteur de données peut les modifier.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```
- Assurez-vous que le JRE qui est utilisé par le serveur d'applications est l'une des versions suivantes :
  - IBM JRE 1.6.0 SR16 FP3 ou version supérieure
  - IBM JRE 1.6.1 SR8 FP3 ou version supérieure
  - IBM JRE 1.7.0 SR8 FP10 ou version supérieure
  - IBM JRE 1.7.1 SR2 FP10 ou version supérieure
  - IBM JRE 1.8 ou version supérieure
  - Autre IBM JRE d'une version supérieure à 1.6.0 SR7 avec le correctif temporaire pour l'APAR IV67574

Pourquoi et quand exécuter cette tâche

La fonction de surveillance des fuites de mémoire nécessite le composant IBM Health Center du JRE d'IBM. Vous devez vous assurer que le JRE qui est utilisé par le serveur d'applications est pris en charge par cette fonction.

- Sur les systèmes AIX ou Linux, lorsque vous configurez le collecteur de données de façon à activer la collecte de données de diagnostic, si le JRE en cours est pris en charge, l'utilitaire de configuration vérifie automatiquement si le composant Health Center est admissible et le met à niveau s'il ne l'est pas.
- Sur les systèmes Windows, vous devez mettre à niveau le composant Health Center manuellement si la version en cours n'est pas prise en charge car l'utilitaire de configuration ne peut pas remplacer les fichiers pour un JRE en cours d'exécution.

A faire : La procédure suivante est requise uniquement sur les systèmes Windows. Pour les systèmes AIX ou Linux, pour activer la surveillance des fuites de mémoire, vous devez uniquement vous assurer que la version du JRE est prise en charge et que la collecte des données de diagnostic est activée.

Procédure

1. Vérifiez que la version d'IBM Health Center qui est incluse dans le JRE est utilisée par le serveur d'applications.
   a. A l'invite de commande, accédez au répertoire `bin` qui se trouve dans le répertoire de base du JRE.
   b. Entrez `java -Xhealthcenter -version` et appuyez sur Entrée.

   La commande renvoie la version du JRE, ainsi que la version d'IBM Health Center. La fonction de surveillance des fuites de mémoire nécessite IBM Health Center version 3.0.11 ou supérieure.
2. Si la version d'IBM Health Center n'est pas admissible, effectuez une mise à niveau du JRE vers une version qui contient IBM Health Center version 3.0.11 ou supérieure.
3. Exécutez l'utilitaire de configuration ou de reconfiguration du collecteur de données pour activer la collecte de données de diagnostic.
   - Si vous n'avez pas configuré le collecteur de données, utilisez `simpleconfig` ou `config`.
   - Si vous avez configuré le collecteur de données, utilisez l'utilitaire `reconfig`.

   A faire : Si vous avez activé la collecte de données de diagnostic avant la mise à niveau du JRE, vous devez toujours exécuter de nouveau l'utilitaire de configuration de la collecte de données.

Configuration de l'infrastructure PMI

Pour afficher les données de performances dans des tableaux de bord de surveillance opérationnelle, l'infrastructure PMI (Performance Monitoring Infrastructure) de WebSphere Application Server doit être configurée pour collecter les données de performances.

Pourquoi et quand exécuter cette tâche

Utilisez la console d'administration WebSphere pour activer l'infrastructure PMI et définir le niveau PMI sur le système WebSphere Application Server.

L'infrastructure PMI fournit quatre niveaux prédéfinis suivants :

1. Aucun
2. De base
3. Etendu
4. Tous

Vous pouvez utiliser une option personnalisée pour sélectionner les statistiques individuelles que vous souhaiter activer ou désactiver. Chaque niveau inclut les statistiques du niveau immédiatement inférieur.

Pour afficher les données dans les tableaux de bord de surveillance des ressources, les attributs utilisés pour les calculs associés au tableau de bord doivent être inclus dans le niveau sélectionné.

Par défaut, l'Agent WebSphere Applications définit le niveau de l'infrastructure PMI à un niveau suffisamment élevé pour collecter les attributs obligatoires.

Restriction : Pour afficher les données dans certains widgets de groupe Process Server et Transaction Manager, vous devez définir manuellement le niveau PMI. Pour plus d'informations, consultez l'infobulle relative aux widgets de groupe.

Si vous modifiez le niveau PMI dans la console d'administration WebSphere, vous devez vérifier que le niveau est suffisamment élevé pour permettre la collecte des données requises.

Procédure

- Pour activer l'infrastructure PMI sur le serveur d'applications, procédez comme suit :
  1. Dans la console d'administration WebSphere, développez **Surveillance et optimisation**, puis sélectionnez **PMI (Performance Monitoring Infrastructure)**.

2. Dans la liste des serveurs, cliquez sur le nom de votre serveur.
3. Cliquez sur l'onglet Configuration, puis cochez la case **Activation de l'infrastructure PMI**.
4. Cliquez sur **Appliquer** ou sur **OK**.
5. Cliquez sur **Sauvegarder** pour activer l'infrastructure PMI.

- Pour définir l'infrastructure PMI sur le serveur d'applications, procédez comme suit :
  1. Dans la console d'administration WebSphere, développez **Surveillance et optimisation**, puis sélectionnez **Infrastructure PMI**.
  2. Dans la liste des serveurs, cliquez sur le nom de votre serveur.
  3. Cliquez sur l'onglet Configuration et sélectionnez ensuite l'ensemble de statistiques à utiliser : de base, étendu, tous ou personnalisé.
  4. Cliquez sur **Appliquer** ou sur **OK**.
  5. Cliquez sur **Sauvegarder** pour définir le niveau PMI.

  Pour plus d'informations sur le niveau PMI requis pour chaque attribut, voir la section «Dashboard attributes» dans le manuel Agent WebSphere Applications Reference. Les frais généraux de surveillance engendrés par l'activation de la collecte de chaque attribut sont affichés.

Restauration de la configuration du serveur d'applications depuis une sauvegarde

Si vous avez configuré une instance de serveur d'applications autonome pour la collecte de données, manuellement ou à l'aide de l'utilitaire de configuration ou de migration, et que le démarrage du serveur d'applications échoue, vous devez restaurer la configuration du serveur d'applications à partir d'une sauvegarde. Si vous n'avez pas créé de sauvegarde, contactez le support IBM.

Pourquoi et quand exécuter cette tâche

Dans un environnement Network Deployment, si vous avez configuré une instance de serveur d'applications pour la collecte de données manuellement ou avec l'utilitaire de migration ou de configuration et que le démarrage du serveur d'applications échoue, vous disposez des options suivantes :

- Vous pouvez restaurer la configuration du serveur d'applications à partir d'une configuration de sauvegarde. Si vous n'avez pas créé de sauvegarde, contactez le support IBM.
- Vous pouvez annuler manuellement la configuration du collecteur de données. Le gestionnaire de déploiement et l'agent de noeud doivent être démarrés sur le serveur d'applications. Pour plus d'informations, voir «Suppression manuelle de la configuration du collecteur de données depuis une instance de serveur d'applications», à la page 193.

Cette section concerne uniquement les systèmes d'exploitation Windows, UNIX et Linux.

Procédure

Pour appliquer la configuration de sauvegarde à l'aide de la commande **restoreConfig**, utilisez l'une des procédures suivantes :

- Dans un environnement de déploiement hors réseau, exécutez les étapes suivantes :
  1. Recherchez le fichier de configuration sauvegardé.

     Le répertoire par défaut est *rép_principal_cd*/data. S'il existe plusieurs fichiers de sauvegarde, vérifiez la date et l'heure de modification du fichier. Celui-ci doit porter la date et l'heure de la configuration qui a échoué. Si vous n'avez terminé aucune autre configuration de collecteur de données sur le même hôte après l'échec de la configuration, utilisez le fichier le plus récent dans le répertoire.
  2. Arrêtez toutes les instances du serveur d'applications.
  3. Exécutez la commande **restoreConfig** à partir du répertoire *rép_principal_serveur_app*/profiles/*nom_profil*/bin.

     La syntaxe de la commande est la suivante :

– Windows `restoreConfig.bat` *`chemin_complet_vers_fichier_sauvegarde`*

– Linux AIX `./restoreConfig.sh` *`chemin_complet_vers_fichier_sauvegarde`*

Pour plus d'informations sur les arguments de la commande **restoreConfig**, consultez le WebSphere Application Server Knowledge Center.

4. Redémarrez les instances du serveur d'applications.

- Dans un environnement de déploiement réseau, effectuez les étapes suivantes :

1. Recherchez le fichier de configuration sauvegardé.

   Le répertoire par défaut est *`rép_principal_cd`*`/data`. S'il existe plusieurs fichiers de sauvegarde, vérifiez les date et heure de modification du fichier, qui doivent correspondre à celles de la configuration ayant échoué. Si vous n'avez terminé aucune autre configuration de collecteur de données sur le même hôte après l'échec de la configuration, utilisez le fichier le plus récent dans le répertoire.

2. Arrêtez toutes les instances du serveur d'applications.
3. Créez un répertoire temporaire dans n'importe quel chemin d'accès commode (*rép_temporaire*). Sur un système UNIX ou Linux, créez le répertoire temporaire sous le répertoire `/tmp`.
4. Exécutez la commande `restoreConfig` à partir du répertoire *`rép_principal_serveur_app`*`/profiles/`*`nom_profil`*`/bin`.

   La syntaxe de la commande est la suivante :

   – Windows `restoreConfig.bat` *`chemin_complet_vers_fichier_sauvegarde`*

   – Linux AIX `./restoreConfig.sh` *`chemin_complet_vers_fichier_sauvegarde`*

   La commande **restoreConfig** restaure la configuration du serveur d'applications d'origine dans le répertoire temporaire.

5. Copiez les fichiers `server.xml`, `variables.xml` et `pmi-config.xml` du répertoire temporaire dans le système Deployment Manager.
   – Répertoire source : *`répertoire_temp/rép_principal_configuration_restaurée`*`/cells/`*`nom_cellule`*`/nodes/`*`nom_noeud`*`/servers/`*`nom_serveur`*
   – Répertoire cible : *`rép_principal_serveur_app`*`/profiles/`*`nom_profil`*`/config/cells/`*`nom_cellule`*`/nodes/`*`nom_noeud`*`/servers/`*`nom_serveur`*
6. Effectuez une synchronisation de noeud à partir de la console d'administration du gestionnaire de déploiement associée au noeud.
7. Dans la console d'administration du gestionnaire de déploiement, sauvegardez les modifications dans la configuration principale.
8. Démarrez les instances du serveur d'applications.

Configuration du collecteur de données Liberty pour les applications sur site

Pour surveiller le profil Liberty sous Linux for System x, vous pouvez déployer directement un collecteur de données autonome dans votre répertoire Liberty local, sans installer Agent WebSphere Applications.

Avant de commencer

1. Téléchargez le module du collecteur de données `_datacollectors_linux_8.1.4.0.5.tgz` à partir du site Web IBM Passport Advantage. Pour plus d'informations, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
2. Configurez le package du collecteur de données avec les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

3. Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer les collecteurs de données pour l'envoi du trafic à un proxy direct. Pour obtenir des instructions, voir «Configuration des collecteurs de données pour qu'ils communiquent via un proxy direct», à la page 202.
4. La fonction monitor-1.0 est requise par le collecteur de données. Vous pouvez télécharger cette fonction à partir du référentiel de fonctions Liberty à l'aide de la commande **installUtility**. Pour des instructions, consultez la section relative au téléchargement des actifs dans WebSphere Application Server Network Deployment Knowledge Center.
5. Pour que le tableau de bord Analyse de mémoire contienne des données, vous devez activer la collecte d'allocation de mémoire pour le collecteur de données au cours de la configuration. Cette fonction de diagnostic requiert IBM Health Center 3.0.8 ou version ultérieure. Si la version d'IBM Health Center n'est pas éligible, mettez à niveau l'environnement JRE utilisé par le serveur d'applications vers une version contenant IBM Health Center 3.0.8 ou version ultérieure.

   Conseil : Pour vérifier la version d'IBM Health Center incluse dans l'environnement JRE utilisé par le serveur d'applications, accédez au répertoire `bin` dans le répertoire de base JRE et lancez ensuite `java -Xhealthcenter -version`.

Pourquoi et quand exécuter cette tâche

Vous pouvez choisir de configurer manuellement le collecteur de données ou d'utiliser le script de configuration fourni pour configurer le collecteur de données.

Procédure

- Pour configurer manuellement le collecteur de données, extrayez les fichiers du collecteur de données du module de collecteur de données, puis modifiez des fichiers locaux pour le serveur Liberty.
  1. Exécutez la commande suivante pour extraire les fichiers du package de collecteur de données :
     ```
     tar -xzf _datacollectors_linux_8.1.4.0.5.tgz
     ```
     Le module `liberty_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
  2. Extrayez les fichiers du module `liberty_datacollector_8.1.4.0.tgz` dans un répertoire local à l'aide de la commande ci-dessous. Le répertoire extrait devient le répertoire de base du collecteur de données.
     ```
     tar -xzf liberty_datacollector_8.1.4.0.tgz
     ```
     Par exemple, pour extraire les fichiers dans le répertoire `/opt/ibm/apm/`, exécutez les commandes suivantes :
     ```
     cd /opt/ibm/apm
     tar -xzf liberty_datacollector_8.1.4.0.tgz
     ```
     Les fichiers extraits se trouvent dans le répertoire `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.06`. Ce répertoire est appelé répertoire de base du collecteur de données (*base_cd*) dans les étapes ci-après.
  3. Accédez au répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
  4. Editez le fichier `jvm.options` en ajoutant les paramètres ci-après. Si le fichier `jvm.options` n'existe pas, créez-le avec un éditeur de texte.
     ```
     -agentlib:am_ibm_16=nom_serveur
     -Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
     -Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
     -Dliberty.home=base_liberty
     -Xhealthcenter:level=inprocess
     -Xgc:allocationSamplingGranularity=10000
     -verbosegc
     -Xverbosegclog:chemin_accès_absolu_au_fichier_journal,1,10000
     ```
     Lors de l'ajout de ces entrées, notez ce qui suit :

– Chaque entrée doit se trouver sur une ligne distincte.
– Remplacez *nom_serveur* par le nom du serveur Liberty.
– Remplacez *base_cd* par le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.06`.
– Remplacez *base_liberty* par la racine du répertoire d'installation Liberty. Par exemple, `/opt/ibm/wlp`.
– Si le serveur Liberty fonctionne avec une lourde charge de travail, ajoutez le paramètre `-Xmx` pour allouer une taille de segment de mémoire de 512 Mo supplémentaire pour le collecteur de données. Par exemple, `-Xmx1024M`.
– Les lignes `-Xhealthcenter:level=inprocess` et `-Xgc:allocationSamplingGranularity=10000` sont facultatives. Ajoutez les deux lignes uniquement si vous souhaitez activer la collecte d'allocation de mémoire qui est désactivée par défaut. L'activation de cette fonction est nécessaire pour que le tableau de bord Analyse de mémoire contienne des données.
– La ligne `-Xverbosegclog:`*`chemin_accès_absolu_au_fichier_journal`*`,1,10000` est facultative ; elle indique le chemin d'accès au fichier journal de récupération de place redirigé. Si elle n'est pas indiquée, les journaux sont enregistrés dans un fichier qui est renouvelé tous les 10000 échecs d'allocation. Le fichier `stdout` ou `stderr` d'origine (`console.log`) peut être très volumineux lors de l'exécution du serveur. Ajoutez cette ligne si vous souhaitez sauvegarder les fichiers journaux de sortie de récupération de place dans un autre répertoire et limiter le nombre et la taille des fichiers journaux. Si le chemin d'accès indiqué n'est pas valide, cette ligne n'a pas d'effet et le fichier journal de récupération de place reste le fichier `stdout` ou `stderr`.

5. Ouvrez le fichier `server.env` dans le même répertoire et ajoutez le chemin ci-après à l'entrée d'environnement. Si le fichier `server.env` n'existe pas, créez-le avec un éditeur de texte.

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/lib:base_cd/toolkit/lib/lx8266:base_cd/
   toolkit/lib/lx8266/ttapi
   ```

   Lors de l'ajout de ces entrées, notez ce qui suit :
   – Chaque entrée doit se trouver sur une ligne distincte.
   – Remplacez *base_cd* par le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.06`.
6. Modifiez le fichier `server.xml` dans le même répertoire pour activer la fonction de surveillance en ajoutant la ligne suivante à la section `<featureManager>` :

   ```
   <feature>monitor-1.0</feature>
   ```
7. Redémarrez le serveur Liberty.

• Pour configurer le collecteur de données en répondant à des invites, utilisez le script de configuration fourni dans les packages de collecteur de données.

1. Exécutez la commande suivante pour extraire les fichiers du package de collecteur de données :

   ```
   tar -xzf _datacollectors_linux_8.1.4.0.5.tgz
   ```

   Le module `liberty_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
2. Extrayez les fichiers du module `liberty_datacollector_8.1.4.0.tgz` à l'aide de la commande ci-dessous.

   ```
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Par exemple,

   ```
   cd /opt/ibm
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Les fichiers du collecteur de données extraits se trouvent dans le répertoire `liberty_dc`.
3. Accédez au répertoire `liberty_dc/.gdc/7.3.0.14.06/bin` et démarrez le script de configuration en exécutant la commande suivante :

   ```
   ./config_liberty_dc.sh
   ```

4. A l'invite de commande, entrez la racine de votre répertoire d'installation Liberty ou acceptez la valeur par défaut. Par exemple, `/opt/ibm/wlp`.
5. A l'invite, entrez le répertoire de base de la machine virtuelle Java qui est utilisé par le serveur d'applications ou acceptez le répertoire par défaut. Par exemple, `/opt/ibm/java`.
6. Le programme de configuration peut reconnaître et répertorier automatiquement les serveurs d'applications non configurés dans le répertoire spécifié. Entrez le numéro qui correspond au serveur Liberty à configurer. Pour sélectionner plusieurs serveurs, séparez les numéros par un espace ou entrez `*` pour sélectionner tous les serveurs.
7. Une fois que le programme de configuration a terminé de mettre à jour les fichiers de tous les serveurs Liberty, mettez à jour manuellement la taille de segment de mémoire de JVM afin d'allouer un segment de mémoire supplémentaire de 512 Mo pour le collecteur de données.
8. Redémarrez les serveurs pour que la configuration soit prise en compte.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM. La surveillance des ressources, le suivi des transactions et les données de diagnostic sont activées. Toutefois, la collecte de segments de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez les activer avec les fichiers de propriétés du collecteur de données si vous avez besoin des données contenues dans les tableaux de bord Cliché de tas et Analyse de mémoire.

Que faire ensuite

- Pour afficher les données de surveillance de vos serveurs Liberty, démarrez la console Cloud APM. Pour les instructions, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

  A faire : Lorsque vous ajoutez l'instance de collecteur de données Liberty sur le Tableau de bord des applications, sélectionnez **Liberty Runtime** au lieu de **WebSphere Application Server** dans la liste des composants.
- Pour que les tableaux de bord Cliché de tas et/ou Analyse de mémoire contiennent des données, vous devez également activer la collecte des données pour le collecteur d'instantané de segment de mémoire et/ou la collecte d'allocation de mémoire, ce qui est faisable dans les fichiers `.properties` du collecteur de données. Voir «Activation ou désactivation de la collecte des données de suivi des transactions et des données de diagnostic», à la page 818.
- Si le fichier de clés ou le serveur Cloud APM est modifié, reconnectez le collecteur de données au serveur Cloud APM. Pour plus d'informations, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 234.

Configuration avancée du collecteur de données

Vous pouvez éditer les fichiers de configuration du collecteur de données afin de modifier des paramètres de surveillance supplémentaires.

Fichiers de propriétés du collecteur de données Liberty :

Divers fichiers de configuration sont fournis pour que vous puissiez contrôler davantage la configuration et le comportement du collecteur de données.

Une fois que vous avez extrait le package du collecteur de données dans un répertoire local, les fichiers du collecteur de données se trouvent dans le répertoire *rép_local*`/liberty_dc/.gdc/7.3.0.14.06`. Par exemple, `/opt/ibm/apm/.gdc/7.3.0.14.06`. Ce dossier devient le répertoire de base du collecteur de données, qui est appelé *base_cd* dans les instructions qui suivent, par mesure de simplification.

Fichiers de propriétés du collecteur de données

Chaque instance de serveur d'applications surveillée par le collecteur de données possède son propre fichier de propriétés. Le collecteur de données crée automatiquement le fichier de propriétés. Le nom du fichier est *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/datacollector.properties.

Pour faciliter les mises à niveau ultérieures, ne modifiez pas ce fichier.

Ajoutez plutôt les paramètres que vous souhaitez modifier au fichier de propriétés personnalisées du collecteur de données. Ce fichier est nommé *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/datacollector_custom.properties. Les paramètres du fichier de propriétés personnalisées du collecteur de données remplacent les valeurs du fichier de propriétés du collecteur de données.

Important : Si le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/datacollector_custom.properties n'existe pas, créez-le lorsque vous souhaitez effectuer des modifications. Il se peut que vous deviez également créer le répertoire custom.

Fichier de propriétés du kit d'outils

Le fichier de propriétés du kit d'outils est automatiquement créé par le collecteur de données au démarrage, à l'aide de différents fichiers d'entrée. Il est unique pour chaque instance de serveur d'applications surveillée par le collecteur de données. Son nom est *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/toolkit.properties.

Ce fichier étant recréé à chaque démarrage du collecteur de données, **ne lui apportez pas de modifications** car elles seront remplacées.

Ajoutez plutôt les paramètres que vous souhaitez modifier au fichier de propriétés personnalisées du kit d'outils. Ce fichier est nommé *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties. Les paramètres du fichier de propriétés personnalisées du kit d'outils remplacent les valeurs du fichier de propriétés du kit d'outils.

Vous pouvez également définir les propriétés du kit d'outils de toutes les instances de serveur d'applications surveillées par l'installation du collecteur de données. Pour cela, ajoutez les paramètres au fichier de propriétés personnalisées du kit d'outils global : *base_cd*/runtime/custom/toolkit_global_custom.properties. Cependant, si une propriété est définie dans le fichier toolkit_custom.properties propre à l'instance, elle remplace la valeur dans le fichier global pour cette instance.

Important : Si le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties ou *base_cd*/runtime/custom/toolkit_custom.properties n'existe pas, créez-le lorsque vous souhaitez effectuer des modifications. Il se peut que vous deviez également créer le répertoire custom.

Autres fichiers de propriétés

Outre le fichier de propriétés du collecteur de données et le fichier de propriétés du kit d'outils, il existe d'autres fichiers de propriétés propres à chaque instance de serveur d'applications surveillée par le collecteur de données.

base_cd/**runtime**/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/**custom/gdc/gdc_custom.properties**
: Définit les détails de collecte des données de diagnostic et de trace de méthode. Pour plus d'informations sur la modification de ce fichier, voir «Configuration de la collecte d'informations de diagnostic détaillées», à la page 820.

base_cd/**runtime**/*version_serveur_app*.*nom_noeud*.*nom_serveur*/**hc.properties**
: Définit les détails de la collecte d'instantanés de segment de mémoire et de la collecte d'allocation de mémoire. Pour plus d'informations sur la modification de ce fichier, voir «Configuration de la collecte d'informations de diagnostic détaillées», à la page 820.

base_cd/**runtime**/*version_serveur_app*.*nom_noeud*.*nom_profil*.*nom_serveur*/**cynlogging.properties**
: Définit les détails des noms de fichier journal et de la consignation pour la portion Java du collecteur de données.

base_cd/**runtime**/*version_serveur_app*.*nom_noeud*.*nom_profil*.*nom_serveur*/**cyn-cclog.properties**
: Définit les détails des noms de fichier journal et de la consignation pour la portion C++ du collecteur de données.

Fichiers de trace du collecteur de données

Les fichiers de trace du collecteur de données sont stockés par défaut dans les emplacements suivants :

- Windows *base_cd*\logs\CYN\logs.
- Linux AIX *base_cd*/logs/CYN/logs.

Activation ou désactivation de la collecte des données de suivi des transactions et des données de diagnostic :

Par défaut, le suivi des transactions et des méthodes est activé pour le collecteur de données. La collecte des instantanés de segment de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez personnaliser la collecte de données ou les intervalles auxquels les données de diagnostic sont collées en modifiant les fichiers `.properties` du collecteur de données.

Pourquoi et quand exécuter cette tâche

Les fichiers de propriétés du collecteur de données sont dans le répertoire *base_dc*, par exemple `/opt/ibm/apm/.gdc/7.3.0.14.06`. Utilisez les différents fichiers de propriétés pour personnaliser le collecteur de données pour atteindre les objectifs suivants :

- Activation ou désactivation du suivi des transactions.
- Activation ou désactivation de la collecte d'instantanés de segment de mémoire.
- Spécification de l'intervalle auquel le collecteur de données prend un instantané du cliché de tas.
- Activation ou désactivation de la surveillance de l'allocation de mémoire.
- Spécification de l'intervalle auquel le collecteur de données collecte les informations d'allocation de mémoire.
- Activation ou désactivation du suivi des méthodes.

A faire : Selon que vous avez redémarré le serveur Liberty après la configuration du collecteur de données, des fichiers `.properties` différents sont applicables. Si vous avez redémarré le serveur Liberty après la configuration du collecteur de données, un répertoire `runtime` est créé dans le répertoire *base_dc*. Après cela, vous pouvez utiliser uniquement les fichiers `.properties` dans le répertoire *base_dc*`/runtime/`*appserver_version.node_name.profile_name.server_name* pour personnaliser le collecteur de données pour chaque serveur d'applications.

Procédure

- Pour activer ou désactiver le suivi des transactions, définissez la propriété **com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled** dans le fichier suivant sur `true` ou `false` :

  base_dc/runtime/*version_serveur_apps*.*nom_noeud*.*nom_serveur*/ldc.properties (si le répertoire runtime n'existe pas, utilisez *base_dc*/ldc/etc/ldc.properties) Une fois que le suivi des transactions est activé, vous pouvez surveiller la pile d'application IBM Java dans les topologies.
- Pour activer ou désactiver la collecte des instantanés de segment de mémoire, définissez les propriétés **com.ibm.tivoli.itcam.hc.send.heap.enable** et **com.ibm.tivoli.itcam.hc.snapshot.automatic.enable** dans le fichier suivant sur `true` ou `false`.

  base_dc/runtime/*version_serveur_apps*.*nom_noeud*.*nom_serveur*/hc.properties (si le répertoire runtime n'existe pas, utilisez *base_dc*/healthcenter/etc/hc.properties) Une fois que la collecte d'instantanés de segment de mémoire est activée, le collecteur de données peut prendre un instantané de segment de mémoire à intervalles spécifiés. Les informations sur le cliché de tas peuvent être affichées dans le tableau de bord Cliché de tas.
- Pour modifier l'intervalle auquel l'instantané de segment de mémoire est pris par le collecteur de données, définissez la propriété **com.ibm.tivoli.itcam.hc.snapshot.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est `360`.

  base_dc/runtime/*version_serveur_apps*.*nom_noeud*.*nom_serveur*/hc.properties (si le répertoire runtime n'existe pas, utilisez *base_dc*/healthcenter/etc/hc.properties)
- Pour activer ou désactiver la collecte d'allocation de mémoire, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** dans le fichier suivant sur `true` ou `false`.

  base_dc/runtime/*version_serveur_apps*.*nom_noeud*.*nom_serveur*/hc.properties (si le répertoire runtime n'existe pas, utilisez *base_dc*/healthcenter/etc/hc.properties)

  A faire : Pour activer la collecte d'allocation de mémoire, assurez-vous également que les deux lignes suivantes sont ajoutées au fichier jvm.options du serveur Liberty.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

  Une fois que la collecte d'allocation de mémoire est activée, les données sont disponibles dans le tableau de bord Analyse de la mémoire.
- Pour spécifier l'intervalle auquel les informations d'allocation de mémoire sont collectées, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est `15`.

  base_dc/runtime/*version_serveur_apps*.*nom_noeud*.*nom_serveur*/hc.properties (si le répertoire runtime n'existe pas, utilisez *base_dc*/healthcenter/etc/hc.properties)
- Pour activer ou désactiver le suivi des méthodes, définissez la propriété **dfe.enable.methoddata** dans le fichier suivant sur `true` ou `false`:

  base_dc/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc/gdc_custom.properties (si le répertoire runtime n'existe pas, utilisez *base_dc*/gdc/etc/gdc_dfe.properties)

Résultats

Après avoir modifié les fichiers .properties, redémarrez le serveur Liberty pour que la modification soit prise en compte.

Pour plus d'informations sur les fichiers .properties du collecteur de données pour chaque serveur d'applications, voir «Fichiers de propriétés du collecteur de données Liberty», à la page 816.

Que faire ensuite

- Une fois que le suivi des méthodes est activé, vous pouvez définir des seuils pour différents types de demande, afin que des niveaux différents de données de surveillance puissent être collectés pour des demandes différentes. Pour obtenir des instructions, voir «Personnalisation des seuils de demande», à la page 822.
- Si vous avez désactivé la collecte d'allocation de mémoire, n'oubliez pas de supprimer les lignes suivantes du fichier `jvm.options` du serveur Liberty :

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Configuration de la collecte d'informations de diagnostic détaillées :

Si vous disposez d'IBM Cloud Application Performance Management, Advanced Private, vous pouvez utiliser le collecteur de données pour collecter des informations de diagnostic détaillées sur l'instance de serveur d'applications surveillée. Pour configurer le comportement de la collecte des données de diagnostic, notamment la quantité d'informations de diagnostic stocké par le collecteur de données, personnalisez le fichier de configuration `gdc_custom.properties`.

Pourquoi et quand exécuter cette tâche

Le fichier `gdc_custom.properties` se trouve dans le répertoire *rép_base_cd*`/runtime/`*version_serveurapp.nom_noeud.nom_profi.nom_serveur*`/custom/gdc`.

Les exemples suivants expliquent comment utiliser les propriétés du fichier de configuration `gdc_custom.properties` pour effectuer les opérations suivantes :

- Définition des limites relatives à la taille et au nombre des fichiers d'informations détaillés
- Définition de la collecte complète ou partielle des données de demande et des données de diagnostic de méthode

Vous pouvez également définir d'autres propriétés dans le fichier `gdc_custom.properties` pour personnaliser la collecte de données de diagnostic. Reportez-vous aux commentaires du fichier qui décrivent les propriétés.

A faire : Après avoir modifié le fichier `gdc_custom.properties`, vous devez redémarrer l'instance de serveur d'applications surveillée pour appliquer les modifications.

Définition des limites relatives à la taille et au nombre des fichiers d'informations détaillés :
Pourquoi et quand exécuter cette tâche

Le collecteur de données stocke les informations de diagnostic dans un certain nombre des fichiers. Par défaut, il stocke 100 fichiers ; si 100 fichiers sont déjà stockés et qu'un nouveau fichier est créé, le fichier le plus ancien est supprimé. Le collecteur de données crée un nouveau fichier toutes les 15 minutes, ou lorsque la taille du fichier en cours dépasse 200 mégaoctets. Lorsque la taille totale du répertoire contenant les fichiers dépasse 2 gigaoctets, le collecteur de données supprime le fichier le plus ancien.

Procédure

Vous pouvez changer les paramètres suivants dans le fichier *rép_principal_collecteur_données*`/runtime/`*version_serveur_applications.nom_noeud.nom_profil.nom_serveur*`/custom/gdc/gdc_custom.properties` :

- Pour définir le nombre maximal de fichiers contenant des informations de diagnostic, définissez la propriété `com.ibm.itcam.gdc.dfe.filelimit`. Par exemple :

```
com.ibm.itcam.gdc.dfe.filelimit=100
```

- Pour définir le délai, en minutes, après lequel le collecteur de données crée un nouveau fichier de données de diagnostic, définissez la propriété `com.ibm.itcam.gdc.dfe.frequency`. Par exemple :

  ```
  com.ibm.itcam.gdc.dfe.frequency=15
  ```

- Pour définir la taille maximale des fichiers de données de diagnostic, en mégaoctets, définissez la propriété `dfe.file.maxlimit`. Par exemple :

  ```
  dfe.file.maxlimit=200
  ```

  Si les fichier de données de diagnostic en cours atteint cette taille, le collecteur de données crée un nouveau fichier de données de diagnostic.

- Pour définir la taille totale maximale de tous les fichiers de données, en mégaoctets, définissez la propriété `trace.dir.size.limit`. Par exemple :

  ```
  trace.dir.size.limit=2147483648
  ```

  Si la somme des tailles de tous les fichiers de données de diagnostic dépasse cette valeur, le collecteur de données supprime le fichier de données le plus ancien. La taille totale minimale est de 25 mégaoctets.

Définition de la collecte complète ou partielle des données de demande et des données de diagnostic de méthode :
Pourquoi et quand exécuter cette tâche

Le collecteur de données a les paramètres par défaut suivants :

- Le collecteur de données ne collecte les données de diagnostic que pour les demandes sélectionnées. La sélection (l'échantillon) des demandes vise à inclure toutes les erreurs et certaines demandes correctes.
- La collecte des données de méthode est désactivée au démarrage du serveur.
- Lorsque la collecte des données de méthode est activée, le collecteur de données récupère les données de méthode pour certaines demandes uniquement (de celles pour lesquelles les données de diagnostic sont collectées). Cette sélection avancée (échantillon) vise de nouveau à inclure toutes les erreurs et certaines demandes correctes.

Important : La modification de ces paramètres affecte le performance du serveur d'application. Sur les serveurs de production, la dégradation de la performance peut être critique.

Procédure

Vous pouvez modifier ces paramètres à l'aide des propriétés dans le fichier *rép_base_cd*`/runtime/`*version_serveurapplications.nom_noeud.nom_profil. nom_serveur*`/custom/gdc/gdc_custom.properties`.

- Pour activer la collecte des méthodes de données au démarrage du serveur, définissez la propriété de la manière suivante :

  ```
  dfe.enable.methoddata=true
  ```

  Conseil : Vous pouvez utiliser la page Configuration d'agent pour activer ou désactiver de manière dynamique la collecte des données de trace de méthode.

- Pour collecter les données de diagnostic pour toutes les demandes, désactivez l'échantillonnage en définissant la propriété de la manière suivante :

  ```
  dc.sampling.enable=false
  ```

- Pour activer la collecte des données de méthode pour toutes les demandes dont les données de diagnostic sont collectées, définissez la propriété de la manière suivante :

  ```
  dc.sampling.enable=false
  dc.sampling.methsampler.enabled=false
  ```

  A faire : La propriété `dc.sampling.methsampler.enabled` prend effet uniquement lorsque la collecte des données de méthode est activée dans la page de configuration d'agent ou par la propriété `dfe.enable.methoddata`.

Personnalisation des seuils de demande :

Certaines demandes peuvent ne pas avoir suffisamment d'informations si les seuils par défaut sont élevés. Vous pouvez personnaliser les seuils de demande afin que davantage de demandes ou de données contextuelles de demande puissent être capturées par le collecteur de données.

Pourquoi et quand exécuter cette tâche

Chaque type de demande comporte deux types de seuil, qui sont nommés **perfThreshold** et **secondaryPerfThreshold**. Une demande est capturée par le collecteur de données uniquement quand elle est plus longue que la durée spécifiée pour le seuil **perfThreshold**. Les données contextuelles, comme la trace de la pile et l'instruction SQL, sont capturées uniquement lorsque la demande prend plus de temps que la durée spécifiée pour le seuil **secondaryPerfThreshold**. Vous pouvez ajuster ces valeurs de seuil en fonction de vos besoins.

Procédure

1. Accédez au répertoire *base_cd*\gdc\etc, *base_cd* correspondant au répertoire de base du collecteur de données.
2. Dans un éditeur de texte, ouvrez le fichier XML pour le type de demande que vous souhaitez personnaliser. Vous pouvez dire quel fichier est pour quel type de demande d'après le nom du fichier XML. Par exemple, le fichier `ejb.xml` concerne les demandes d'EJB, le fichier `custom.xml` concerne les demandes personnalisées et le fichier `appMethods.xml` concerne la classe et les méthodes lorsque la trace de méthode est activée.
3. Définissez les balises `<collectContextData>`, `<collectStackTrace>` et `<createDataRow>` sur `ifThresholdExceeded`.

   ```
   <collectContextData>ifThresholdExceeded</collectContextData>
   <collectStackTrace>ifThresholdExceeded</collectStackTrace>
   <createDataRow>ifThresholdExceeded</createDataRow>
   ```

4. Définissez les balises `<perfThreshold>` et `<secondaryPerfThreshold>` sur les valeurs de seuil de votre choix. L'unité du seuil est la milliseconde. Par exemple, le fichier `ejb.xml` a les paramètres suivants pour les demandes d'EJB. En conséquence, seules les demandes d'EJB qui prennent plus de 1 seconde (1000 millisecondes) sont capturées par le collecteur de données. En outre, les données contextuelles liées à une demande d'EJB, comme la trace de la pile et l'accueil d'EJB, sont capturées uniquement lorsque la demande d'EJB prend plus de 1,5 secondes (1500 millisecondes).

   ```
   <requestProbePoint id="EJB">
   <interface>com.ibm.tivoli.itcam.toolkit.ai.boot.aspectmanager.ITurboEJBEventListener</interface>
   <family>EJB</family>
   <collectContextData>ifThresholdExceeded</collectContextData>
   <collectStackTrace>ifThresholdExceeded</collectStackTrace>
   <perfThreshold>1000</perfThreshold>
   <secondaryPerfThreshold>1500</secondaryPerfThreshold>
   <dataToCollect>instanceAndSummary</dataToCollect>
   <createDataRow>ifThresholdExceeded</createDataRow>
   <requestType>EJB Method</requestType>
   </requestProbePoint>
   ```

5. Sauvegardez vos changements, puis redémarrez le serveur d'applications.

Désactivation des divers types d'instrumentation par code intermédiaire des API Java EE :

Dans BCI (Byte Code Instrumentation), le collecteur de données intercepte les appels des entrées et des sorties de différents types d'API Java Platform Enterprise Edition (Java EE) afin de créer un flux d'exécution pour chaque demande d'application. Des ressources sont utilisées pour la surveillance. Vous pouvez paramétrer le collecteur de données afin d'exclure certaines de ces API de la surveillance et réduire ainsi la consommation de ressources.

Pour désactiver la surveillance BCI pour les API Java EE, ajoutez les propriétés suivantes au fichier de propriétés personnalisées du kit d'outils. Pour plus d'informations sur ce fichier, voir «Fichier de propriétés du kit d'outils», à la page 817.

Tableau 191. Ajout de lignes au fichier de propriétés personnalisées du kit d'outils

Type d'API Java EE	**Ligne à ajouter au fichier `toolkit_custom.properties`**
Enterprise JavaBeans (EJB)	`com.ibm.tivoli.itcam.toolkit.ai.enableejb=false`
Java Connector Architecture (JCA)	`com.ibm.tivoli.itcam.toolkit.ai.enablejca=false`
Java Database Connectivity (JDBC)	`com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false`
Java Naming and Directory Interface (JNDI)	`com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false`
Java Message Service (JMS)	`com.ibm.tivoli.itcam.toolkit.ai.enablejms=false`
Conteneurs Web pour Servlets/Pages JSP (JavaServer Pages)	`com.ibm.tivoli.itcam.dc.was.webcontainer=false`
Suivi du nombre de sessions HTTP	`com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false`
CICS Transaction Gateway (CTG)	`com.ibm.tivoli.itcam.dc.ctg.enablectg=false`
IMS	`com.ibm.tivoli.itcam.dc.mqi.enableims=false`
Java Data Objects (JDO)	`com.ibm.tivoli.itcam.dc.mqi.enablejdo=false`
MQI (Message Queue Interface)	`com.ibm.tivoli.itcam.dc.mqi.enablemqi=false`
Service Web Axis	`com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false`
RMI (Remote Method Invocation)	`am.ejb.rmilistener.enable=false`
Conteneur d'EJB WebSphere Application Server	`com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false`

Personnalisation du mappage des informations des demandes :

Dans certains cas, il peut être nécessaire de changer les informations qui identifient les demandes surveillées par l'agent. Ces informations incluent le nom de la demande et toutes les données qui peuvent être affichées pour la demande (par exemple, le texte de la requête pour une requête SQL). Pour modifier ces informations, vous devez définir une configuration d'associateur de demande personnalisée.

Pourquoi et quand exécuter cette tâche

Pour personnaliser le mappage des informations de demande, vous devez définir une configuration d'associateur de demande personnalisée dans un fichier XML.

Dans ce fichier, certains des *symboles* intégrés représentent les valeurs du contexte d'exécution de la demande. Vous pouvez créer des symboles supplémentaires, qui calculent de nouvelles valeurs. Le calcul peut inclure des valeurs de demande d'origine, des expressions, des appels à des méthodes Java (y compris les méthodes présentes dans l'application surveillée), des conditions et des itérations sur un ensemble de valeurs.

Puis, vous pouvez *mapper* le contenu des symboles dans les nouvelles données de demande qui sont fournies au serveur Cloud APM. Si une variable dans les données de demande n'est pas mappée, la valeur d'origine est conservée.

Dans la mesure où des données différentes sont collectées selon les types de demandes, une configuration d'associateur de demande personnalisée doit être spécifique à un type de demande donné. Vous pouvez configurer différents associateurs de demande pour différents types de demande sur le même collecteur de données.

Procédure

Pour définir une configuration d'associateur de demande personnalisée pour un type de demande, procédez comme suit :

1. Vous définissez une configuration d'associateur de demande personnalisée dans un fichier XML. Pour plus d'informations sur la syntaxe XML, voir «Syntaxe du fichier XML».
2. Placez le fichier XML dans le répertoire *base_dc*/runtime/custom pour l'employer pour toutes les instances du serveur d'applications, ou dans le répertoire *base_dc*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom pour l'utiliser pour une instance de serveur d'applications.
3. Activez le mappage de demande personnalisée pour ce type dans le fichier de configuration personnalisée du kit d'outils, toolkit_custom.properties ou toolkit_global_custom.properties. Pour obtenir des instructions, voir «Activation d'un associateur de demande», à la page 834.
4. Mettez en référence le fichier XML que vous avez défini à partir du même fichier de configuration personnalisée du kit d'outils. Pour obtenir des instructions, voir «Activation d'un associateur de demande», à la page 834.

Syntaxe du fichier XML :

Le fichier XML que vous créez pour la configuration de l'associateur de demande doit être un code XML valide et doit rester disponible lorsque la configuration est en cours d'utilisation. Placez le fichier XML dans le répertoire *base_dc*/runtime/custom pour l'employer pour toutes les instances du serveur d'applications, ou dans le répertoire *base_dc*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom pour l'utiliser pour une instance de serveur d'applications.

Niveau supérieur

La balise de niveau supérieur est <gpe>. Dans cette balise, utilisez la balise >runtimeConfiguration<. Ces balises n'ont pas d'attributs.

Dans la balise <runtimeConfiguration>, créez une balise <requestMapperDefinition>. Cette balise doit avoir un attribut type. Définissez-la sur le nom du type d'associateur de demande pour le type de demande requis. Pour plus d'informations, voir tableau 193, à la page 837.

Dans la balise <requestMapperDefinition>, les deux balises suivantes doivent être présentes :

<symbolDefinitions>
Contient toutes les définitions des symboles. Les symboles représentent les valeurs que calcule l'agent chaque fois qu'une demande de ce type est détectée.

<selection>
Contient le mappage des clés de contexte aux valeurs. Les clés représentent les données personnalisées envoyées à l'agent. Elles sont prédéfinies pour chaque type de demande. Le mappage peut être conditionnel.

Pour plus d'informations sur les propriétés d'activation et les noms de type de l'associateur de demande, voir tableau 193, à la page 837.

En outre, dans la balise <runtimeConfiguration>, vous pouvez créer une balise <requestMapperClassPath>. Cette dernière permet de définir des fichiers .jar. Dans ces fichiers .jar, vous pouvez référencer des classes Java dans des définitions d'associateur de demande.

Définition d'une expression :

Pour définir des symboles, vous devez utiliser des expressions. L'agent évalue les expressions pour affecter des valeurs aux symboles.

Utilisation de données dans une expression

Une expression peut utiliser les données suivantes :
- Les symboles de données d'entrée pour le type de demande
- D'autres symboles décrits dans la même définition d'associateur de demande
- Des constantes numériques
- Des constantes de type chaîne (délimitées par ", par exemple `"string"`)
- Des constantes booléennes (`true`, `TRUE`, `false`, `FALSE`)
- La constante `null`

Pour plus d'informations sur les symboles de données d'entrée, voir tableau 194, à la page 838.

Si la valeur d'un symbole est une instanciation d'une classe Java, les expressions peuvent contenir des références à des zones et à des méthodes qui sont définies dans la classe. Pour faire référence à une zone, utilisez *`symbole.nom_zone`*. Pour faire référence à une méthode, utilisez *`symbole.nom_méthode(paramètres)`*. L'appel de méthode doit renvoyer une valeur. Par exemple, vous pouvez utiliser les méthodes de chaîne Java avec un symbole ayant une valeur de type chaîne.

Pour faire référence à une zone statique ou à la méthode d'une classe, vous pouvez également utiliser *`nom_classe.nom_zone`* et *`nom_classe.nom_méthode(paramètres)`*.

Si un symbole fait référence à un objet de type tableau, l'expression peut sélectionner un élément (*`symbole[sélecteur]`*) et déterminer la longueur du tableau (*`symbole`*`.length`).

Opérateurs

Vous pouvez utiliser les opérateurs suivants dans une expression :
- Opérateurs booléens : `AND`, `&`, `OR`, `|`, `NOT`, `!`
- Comparaison : `==`, `!=`, `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`
- Opérateurs numériques : `+`, `-`, `*`, `/`
- Parenthèses pour forcer l'ordre d'évaluation : `(`, `)`

Important : Vous devez mettre en échappement les symboles <, > et & dans le code XML. A défaut, vous pouvez utiliser les opérateurs `GT` (supérieur à), `GE` (supérieur ou égal à), `LT` (inférieur à), `LE` (inférieur ou égal à) et `AND`.

L'expression peut évaluer si une valeur est une instance d'une classe, en utilisant l'opérateur `instanceof` :
`expression` `instanceof` *`nom.classe.java`*

Cet opérateur, semblable à l'opérateur Java `instanceof`, génère une valeur booléenne. Dans cet exemple, la valeur est true si la classe à laquelle la valeur *expression* appartient remplit l'une des conditions suivantes :
- Se nomme *`nom.classe.java`*
- Est une sous-classe directe ou indirecte de la classe identifiée par *`nom.classe.java`*.

- Implémente, directement ou indirectement, l'interface identifiée par *nom.classe.java*.

L'expression peut également instancier un nouvel objet d'une classe Java en utilisant l'opérateur `new`. Cet opérateur est similaire à l'opérateur Java `new` :

```
new nom.classe.java(expression1, expression2, ... expressionN)
```

Ordre de priorité des opérateurs

Les opérateurs sont évalués selon un ordre de priorité. Les opérateurs ayant le même niveau de priorité sont évalués de gauche à droite. Vous pouvez modifier l'ordre d'évaluation en utilisant des parenthèses `(` et `)`.

L'ordre de priorité est le suivant :

1. `.` opérateur (appel de méthode ou référence de zone)
2. `[ ]` (sélecteur d'élément de tableau)
3. `new`
4. `!`, `NOT`
5. `*`, `/`
6. `+`, `-`
7. `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`, `instanceof`
8. `==`, `!=`
9. `AND`, `&`
10. `OR`, `|`

Exemple

```
$s1 >= ( 2 * ($s2.sampMethod($s3, true) + 1))
```

L'agent évalue cette expression de la manière suivante :

1. Le symbole `$s1` est évalué. Il doit renvoyer une valeur numérique.
2. Le symbole `$s2` est évalué. Il doit renvoyer un objet Java.
3. Le symbole `$s3` est évalué.
4. La méthode `sampMethod` est appelée pour l'objet qui résulte de l'évaluation de `$s2`. Le résultat de l'évaluation de `$s3` est transmis en tant que premier paramètre et la valeur booléenne `true` est transmise en tant que second paramètre. L'appel de la méthode `sampMethod` doit renvoyer une valeur numérique.
5. 1 est ajouté au résultat de l'étape 4.
6. Le résultat de l'étape 5 est multiplié par 2.
7. Le résultat de l'étape 1 est comparé au résultat de l'étape 6. Si le résultat de l'étape 1 est supérieur ou égal au résultat de l'étape 6, `true` est renvoyé. Sinon, c'est la valeur `false` qui est renvoyée.

Définition des symboles de base :

Pour définir des symboles, vous devez utiliser des expressions. L'agent évalue les expressions pour affecter des valeurs aux symboles.

Dans la balise <symbol>, utilisez les balises suivantes :

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<eval>
Expression que l'agent doit évaluer pour produire la valeur de ce symbole. Pour plus d'informations sur la définition des expressions, voir «Définition d'une expression», à la page 825.

<type>
Type de la valeur renvoyée par le symbole. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. La définition du type de symbole est facultative. S'il n'est pas défini, l'associateur de demande essaye d'établir le type de zone en fonction de l'expression. Si l'associateur de demande ne peut pas déterminer le type de symbole avant qu'il évalue l'expression, les performances sont affectées. Pour optimiser les performances, il est donc préférable de spécifier le type.

<args>
Arguments associés au symbole. Cette balise est facultative ; si elle est définie, des arguments doivent être fournis pour calculer le symbole. Pour plus d'informations, voir «Définition des arguments de symbole».

Exemple

```
<symbol>
   <name>$doubles1</name>
   <eval>$s1*2</eval>
   <type>int</type>
</symbol>
```

Ce symbole renvoie le double de la valeur d'un autre symbole, `$s1`.

Définition des arguments de symbole

Dans la balise <args> de la définition d'un symbole, vous pouvez définir les types d'arguments du symbole.

Dans cette balise, utilisez la balise <type> pour définir les types d'arguments. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. Vous pouvez indiquer plusieurs balises >type< ; chacune de ces balises définit un argument.

Dans ce cas, le symbole doit être référencé avec des arguments entre parenthèses, comme suit :
`$`*`symbol`*`(`*`argument1`*`,`*`argument2`*`...)`

Le nombre d'arguments doit être identique au nombre de définitions de type d'argument.

Dans la définition de symbole, le premier argument correspond à `$p0`, le second argument correspond à `$p1`, etc.

Un symbole avec des arguments fonctionne comme une méthode Java. L'expression utilise les arguments comme des entrées et renvoie une valeur qui dépend des valeurs des arguments.

Exemple

```
<symbol>
   <name>$double</name>
   <eval>$p0*2</eval>
   <type>int</type>
   <args>
       <type>int</type>
   </args>
</symbol>
```

Ce symbole renvoie le double de la valeur de l'argument. Pour l'évaluer, indiquez un argument numérique : `$double(2)`, `$double($s1)`.

Définition de symboles d'itération :

Dans la balise <symbolDefinitions>, vous pouvez définir un symbole d'itération à l'aide de la balise <iterationSymbol>. Un symbole d'itération représente une valeur qui est acquise par itération à travers un ensemble d'objets dans un tableau, une énumération ou une collection Java. Pour chacun des membres, l'associateur de demande évalue une ou plusieurs expressions de condition. Si une expression renvoie `true`, l'associateur de demande utilise le membre pour calculer la valeur de retour. Quand un membre respecte l'expression de condition, l'associateur de demande n'évalue pas le reste des membres.

Dans la balise <iterationSymbol>, insérez les balises suivantes :

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère `$`.

<type>
Type de la valeur renvoyée par le symbole. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. La définition du type de symbole est facultative. S'il n'est pas défini, l'associateur de demande essaye d'établir le type de zone en fonction de l'expression. Si l'associateur de demande ne peut pas déterminer le type de symbole avant qu'il évalue l'expression, les performances sont affectées. Pour optimiser les performances, il est donc préférable de spécifier le type.

<args>
Arguments associés au symbole. Cette balise est facultative ; si elle est définie, des arguments doivent être fournis pour calculer le symbole. Pour plus d'informations, voir «Définition des arguments de symbole», à la page 827.

<iterate over="*expression*">
Définit l'objet (tableau, énumération ou collection) qui contient les membres à itérer. L'expression doit renvoyer un objet du même type. L'associateur de demande itère sur ses membres jusqu'à ce que l'un d'entre eux provoque une expression de condition pour renvoyer `true`, ou qu'il ne reste plus de membre. Définissez les expressions d'itération dans les balises imbriquées dans cette balise, comme suit :

<test>
Définissez la condition et l'expression de retour dans cette balise. Une balise <iterate> peut contenir plusieurs balises <test>. Dans ce cas, l'associateur de demande les évalue tous. Si une expression de condition est vraie, le symbole retourne une valeur en utilisant l'expression de résultat dans la même balise <test> et aucune autre évaluation n'est exécutée.

<castTo>
Facultatif : si cette balise est présente, indiquez-y le nom d'un type Java sous la forme d'un nom de classe Java complet ou d'une primitive Java. L'associateur de demande transtype l'élément itéré dans ce type avant d'évaluer les expressions de condition et de retour. Si cette balise n'est pas présente, l'associateur de demande transtype un membre d'un tableau sur le type de base du tableau, et un membre d'une énumération ou d'une collection sur `java.lang.Object`. Pour un membre de tableau, le type de base du tableau est généralement le bon choix ; donc utilisez cette balise pour que l'associateur de demande itère sur une énumération ou une collection.

<condition>
Expression qui doit renvoyer une valeur booléenne. Utilisez `$iterElement` pour faire référence à l'élément itéré.

<return>
Si l'expression de la balise <condition> renvoie `true`, l'associateur de demande évalue l'expression dans la balise <return>. Le symbole d'itération renvoie la valeur que cette expression génère. Utilisez `$iterElement` pour faire référence à l'élément itéré.

<defaultValue>

Facultatif. Si l'associateur de demande a itéré sur tous les membres de l'objet, mais aucune expression de condition n'a renvoyé `true`, l'associateur de demande évalue l'expression dans la balise >defaultValue<. Le symbole d'itération retourne la valeur qui génère l'expression. Si cette balise est absente, la valeur par défaut renvoyée est `null`.

Exemples

```
<iterationSymbol>
  <name>$userNameCookieValue</name>
  <iterate over="$httpServletRequest.getCookies()">
     <test>
        <condition>$iterElement.getName().equals("userName")</condition>
        <return>$iterElement.getValue()</return>
     </test>
   </iterate>
</iterationSymbol>
```

Ce symbole recherche le cookie nommé "username" et renvoie sa valeur. `$httpServletRequest.getCookies()` renvoie un tableau, dans quel cas l'élément <castTo> est inutile.

```
<iterationSymbol>
  <name>$headerNameStartingWithA</name>
  <iterate over="$httpServletRequest.getHeaderNames()">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.startsWith("A")</condition>
       <return>$iterElement</return>
    </test>
  </iterate>
</iterationSymbol>
```

Ce symbole recherche l'en-tête dont le nom commence par "A" et retourne son nom. `$httpServletRequest.getHeaderNames()` renvoie une énumération, dans quel cas l'élément <castTo> est obligatoire.

```
<iterationSymbol>
  <name>$determined_gender</name>
  <iterate over="$children">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("garçon")</condition>
       <return>"C'est un garçon"</return>
    </test>
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("fille")</condition>
       <return>"C'est une fille"</return>
    </test>
  </iterate>
  <defaultValue>"inconnu"</defaultValue>
</iterationSymbol>
```

Ce symbole itère `$children`, qui doit être un tableau, une énumération ou une collection de chaînes. Si l'une des chaînes contient "garçon", l'expression renvoie "C'est un garçon". Si l'une des chaînes contient "fille", l'expression renvoie "C'est une fille". Enfin, si aucune chaîne dans l'objet `$children` ne contient "garçon" ou "fille", l'expression renvoie la chaîne "inconnu".

Définition de symboles conditionnels :

Dans la balise <symbolDefinitions>, vous pouvez définir un symbole conditionnel à l'aide de la balise <conditionalSymbol>. Un symbole conditionnel représente une valeur acquise en évaluant une série d'expressions conditionnelles. Si une expression renvoie `true`, l'associateur de demande utilise le membre pour calculer la valeur de retour. Lorsqu'un membre rencontre l'expression de condition, l'associateur de

demande évalue une expression de retour correspondante et renvoie le résultat. Une fois que l'associateur de demande trouve un résultat à renvoyer, il n'évalue pas d'autres d'expressions.

Dans la balise <conditionalSymbol>, utilisez les balises suivantes.

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<type>
Type de la valeur renvoyée par le symbole. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. La définition du type de symbole est facultative. S'il n'est pas défini, l'associateur de demande essaye d'établir le type de zone en fonction de l'expression. Si l'associateur de demande ne peut pas déterminer le type de symbole avant qu'il évalue l'expression, les performances sont affectées. Pour optimiser les performances, il est donc préférable de spécifier le type.

<args>
Arguments associés au symbole. Cette balise est facultative ; si elle est définie, des arguments doivent être fournis pour calculer le symbole. Pour plus d'informations, voir «Définition des arguments de symbole», à la page 827.

<if condition="*expression*">
L'attribut `condition` définit une expression de condition à calculer. L'expression doit renvoyer une valeur booléenne. Si la valeur est `true`, l'associateur de demande utilise le contenu de la balise <if> pour essayer de déterminer la valeur de retour. La balise <if> doit contenir l'un ou l'autre des contenus suivants, mais pas les deux :

- Une balise <return>. Cette balise contient une expression. Si l'expression de condition est vraie, l'associateur de demande évalue l'expression et renvoie le résultat.
- N'importe quel nombre de balises <if> imbriquées dans la balise <if>. Si l'expression de condition est vraie, l'associateur de demande traite les balises <if> imbriquées de la même manière qu'une balise <if> de haut niveau. En d'autres termes, il calcule l'expression dans l'attribut `condition` et si l'expression est vraie, il utilise le contenu de la balise et tente de déterminer la valeur de retour.

Important : Si une valeur de retour est déterminée, l'associateur de demande n'évalue pas d'autres expressions. Cependant, si une expression de condition contenue dans une balise <if> est satisfaite mais qu'elle contient d'autres balises <if> imbriquées et qu'aucune des expressions de condition associées n'est vérifiée, l'agent ne renvoie alors aucune valeur. Dans ce cas, l'associateur de demande continue à évaluer les expressions suivantes.

<defaultValue>
Facultatif. Si l'associateur de demande a évalué toutes les expressions de condition, mais qu'aucune n'a renvoyé `true`, l'associateur de demande évalue l'expression de la balise <defaultValue>. Le symbole conditionnel renvoie la valeur produite par l'expression. Si cette balise est absente, la valeur par défaut renvoyée est `null`.

Exemple

```
<symbol>
  <name>$GET</name>
  <eval>"GET"</eval>
</symbol>
<symbol>
  <name>$PUT</name>
  <eval>"PUT"</eval>
</symbol>
<conditionalSymbol>
  <name>$sessionAttribute</name>
  <if condition="$httpServletRequest.getSession(false) != null>
     <if condition="$httpServletRequest.getSession(false).getAttribute($GET)
!= null">
       <return>$httpServletRequest.getSession(false).getAttribute($GET)</return>
```

```
    </if>
    <if condition="true">
      <return>$httpServletRequest.getSession(false).getAttribute($PUT)</return>
     </if>
  </if>
</conditionalSymbol>
```

Ce symbole est supposé être une partie de l'associateur de demande de servlet. Tout d'abord, il vérifie si une session HTTP existe pour le servlet, sinon, le symbole renvoie `null`. Si une session est présente, le symbole vérifie si le servlet possède un attribut GET et renvoie la valeur de cet attribut. Sinon, il renvoie la valeur de l'attribut PUT. Si la deuxième expression de condition a pour résultat true, cette valeur est utilisée comme une clause else. Si la première condition est true, l'associateur de demande n'évalue pas d'autres expressions ; sinon, il poursuit vers la deuxième expression.

Définition des symboles de classe externe :

Dans la balise <symbolDefinitions>, vous pouvez définir une classe externe à l'aide de la balise <externalClassSymbol>. Un symbole de classe externe représente une classe Java externe. La définition d'un symbole de classe externe est facultative car vous pouvez utiliser des classes Java externes directement dans les expressions. Toutefois, il pourrait améliorer la lisibilité de la configuration de l'associateur de demande.

Dans la balise <externalClassSymbol>, insérez les balises suivantes :

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<className>
Nom de la classe définie par le client.

Important : Pour faire référence à une classe Java dans la configuration de l'associateur de demande, que ce soit dans une définition de symbole de classe externe ou dans une expression, vous devez ajouter le chemin complet et le nom du fichier JAR qui contient la classe à la balise <requestMapperClassPath> dans la balise <runtimeConfiguration>.

Une fois que vous avez défini un symbole de classe externe, vous pouvez faire référence à cette classe par le nom du symbole. Vous pouvez également consulter les méthodes et les zones statiques de la classe en utilisant le symbole.

Exemple

```
<externalClassSymbol>
  <name>$rand</name>
  <className>user.class.Random</className>
</externalClassSymbol>
```

Ce symbole fait référence à une classe écrite par l'utilisateur en générant un nombre aléatoire. Le chemin d'accès complet et le nom du fichier JAR qui contient cette classe doivent être présents dans la balise <requestMapperClassPath> au sein de la balise <runtimeConfiguration>.

Pour faire référence à la méthode statique `user.class.Random.generate()` dans une expression, vous pouvez utiliser le symbole externe :

```
$rand.generate()
```

Mappage de valeurs à des clés de contexte :

Dans la balise <requestMapperDefinition>, mappez des valeurs aux clés de contexte à l'aide de la balise <selection>. Ce mappage fournit les modifications dans les informations de surveillance.

Vous pouvez mapper des valeurs aux clés de sortie définies pour le type de demande. Pour plus d'informations, voir tableau 193, à la page 837.

Si aucune valeur n'est mappée à une clé après l'évaluation de la configuration de l'associateur de demande, ITCAM utilise la valeur d'origine extraite de la demande.

Dans la balise <selection>, insérez les balises suivantes.

<matchCriteria>
Expression qui doit renvoyer une valeur booléenne. Le mappage qui est défini dans cette balise est uniquement utilisé si cette expression renvoie `true`.

<mapTo>
Définit une clé et la valeur à lui associer. Dans cette balise, une balise <key> contient la clé et une balise <value> contient la valeur.

<selection>
Vous pouvez imbriquer des balises <selection> les unes dans les autres.

Si des balises <selection> sont imbriquées, le mappage imbriqué est uniquement utilisé si à la fois la première expression <matchCriteria> et les expressions imbriquées renvoient `true`.

Vous pouvez utiliser plusieurs balises <selection> dans une balise <requestMapperDefinition> ou dans une autre balise <selection>. Si une même clé est associée plusieurs fois dans plusieurs balises <selection> au même niveau d'imbrication (c'est-à-dire dans la même balise parent), le premier mappage pour lequel l'expression <matchCriteria> a retourné `true` est utilisé.

Ne mappez pas la même clé à la fois dans la balise <selection> de niveau supérieur et dans les balises imbriquées.

En règle générale, utilisez la valeur <matchCriteria> `true` comme valeur "else" pour la dernière balise "selection" dans un niveau d'imbrication. Si vous souhaitez mapper des valeurs différentes pour différents cas, utilisez plusieurs balises <selection> dans la balise externe ; chacune peut contenir des critères et des valeurs propres à chaque cas particulier. La dernière balise, avec la valeur `true`, prévoit les cas où les informations disponibles ne satisfont aucun des critères.

Exemples

```
<selection>
   <matchCriteria>true</matchCriteria>
   <mapTo>
      <key>Result</key>
      <value>$s1</value>
   </mapTo>
</selection>
```

Dans cette configuration de mappage, `Result` est mappé à la valeur du symbole `$s1`.

```
<matchCriteria>true</matchCriteria>
   <selection>
      <matchCriteria>$b1</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>1</value>
      </mapTo>
   </selection>
   <selection>
      <matchCriteria>true</matchCriteria>
      <mapTo>
```

```
        <key>Result</key>
        <value>2</value>
      </mapTo>
</selection>
```

Dans cette configuration de mappage, le symbole $b1 doit renvoyer une valeur booléenne. Result a pour valeur 1 si $b1 renvoie true et a pour valeur 2 si $b1 renvoie false. Si $b1 renvoie true, l'associateur de demande utilise le mappage pour Result dans la première balise <selection> ; le mappage de la même clé dans la seconde balise n'est pas utilisé.

Définition de demandes personnalisées :

Par défaut, seuls certains types de méthodes et de classes Java sont surveillés par le collecteur de données en tant que demandes. Les servlets, les pages JSP, les méthodes métier à base d'EJB et certaines API Java EE standard sont reconnues comme des demandes. Vous pouvez désigner des classes et méthodes supplémentaires en tant que *demandes personnalisées*.

Pourquoi et quand exécuter cette tâche

Pour activer la surveillance des demandes personnalisées par le collecteur de données, définissez celles-ci dans un fichier XML et définissez la propriété am.camtoolkit.gpe.customxml.custom dans le fichier de propriétés personnalisées du kit d'outils.

Par exemple, le collecteur de données ne reconnaît pas les classes Struts Action en tant que demandes par défaut. Toutefois, vous pouvez configurer des définitions de demande personnalisées afin que les actions soient reconnues comme des demandes imbriquées.

Procédure

Pour activer la surveillance des demandes personnalisées et désigner une ou plusieurs méthodes en tant que demandes personnalisées, procédez comme suit :

1. Effectuez une copie du fichier *base_cd*/itcamdc/etc/custom_requests.xml dans un emplacement temporaire. Ouvrez ensuite la copie du fichier dans un éditeur de texte.
2. Modifiez les paramètres dans le fichier. Le tableau suivant décrit les paramètres modifiables :

Tableau 192. Paramètres du fichier de configuration des demandes personnalisées

Nom de la balise	Description
edgeRequest	Identifie une ou plusieurs méthodes d'application qui doivent être de type BCI (Byte-Code-Instrumented) pour le traitement des demandes personnalisées. La modification des balises requestName, Matches, type et methodName dans la balise edgeRequest permet de personnaliser la sélection. Chaque balise edgeRequest doit contenir précisément une balise methodName et une ou plusieurs balises Matches. Plusieurs balises edgeRequest peuvent être indiquées.
requestName	Définit un nom unique pour cette demande. Le nom de la demande s'affiche pour l'utilisateur lorsque les entrées et les sorties de la méthode sont tracées.
Matches	Identifie une ou plusieurs classes contenant les méthodes qui doivent être de type BCI (Byte-Code-Instrumented) pour le traitement des demandes personnalisées. Il peut y avoir plusieurs balises Matches dans une seule balise edgeRequest.
type	Indique si une classe doit être une classe système ou une classe d'application pour concorder avec la balise edgeRequest.
methodName	Identifie les noms des méthodes dans l'une des classes identifiées par la balise Matches et qui doivent être de type BCI (Byte-Code-Instrumented) pour le traitement des demandes personnalisées. Une seule balise methodName peut être indiquée dans chaque balise edgeRequest.

Tableau 192. Paramètres du fichier de configuration des demandes personnalisées (suite)

Nom de la balise	Description
`requestMapper`	Facultatif. Si cette balise est indiquée, le collecteur de données utilise un associateur de demande afin de déterminer les informations qui identifient la demande. Vous pouvez définir des méthodes non standard pour extraire ces informations. Pour plus d'informations sur l'activation et la définition des associateurs de demande, voir «Personnalisation du mappage des informations des demandes», à la page 823.
A faire : Les balises `Matches` et `methodName` peuvent inclure des caractères génériques. Le mécanisme des caractères génériques est décrit ci-après : • L'astérisque (*) représente zéro, une ou plusieurs occurrences d'un caractère quelconque lorsqu'il est utilisé seul. S'il est imbriqué dans une séquence de caractères (par exemple, `java.*.String`), il représente zéro, une ou plusieurs occurrences d'un caractère quelconque excepté le séparateur de module (.). • Deux points (..) peuvent être utilisés pour définir tous les sous-packages. Ils correspondent à toute suite de caractères commençant et finissant par le séparateur de module (.). Par exemple, `java..String` correspond à `java.lang.String` et `com.ibm..*` correspond à toute déclaration commençant par `com.ibm`.	

Par exemple, une application dont le nom de module est `com.mycompany.myapp` doit remplir les conditions suivantes :

- Dans la classe `Customer`, la méthode `creditCheck()` doit être traitée comme une demande personnalisée appelée `CreditCheck`.
- Dans la classe `Supplier`, la méthode `inventoryCheck()` doit être traitée comme une demande personnalisée appelée `SupplyCheck`.

Le contenu du fichier `custom_requests.xml` personnalisé qui permet de satisfaire ces conditions est le suivant :

```
<customEdgeRequests>
      <edgeRequest>
              <requestName>CreditCheck</requestName>
              <Matches>com.mycompany.myapp.Customer</Matches>
              <type>application</type>
              <methodName>creditCheck</methodName>
      </edgeRequest>
      <edgeRequest>
              <requestName>SupplyCheck</requestName>
              <Matches>com.mycompany.myapp.Supplier</Matches>
              <type>application</type>
              <methodName>inventoryCheck</methodName>
      </edgeRequest>
</customEdgeRequests>
```

3. Effectuer l'une des étapes suivantes :
   - Sauvegardez le fichier dans le répertoire *base_cd*`/runtime/`*version_serveur_app.nom_noeud.nom_profil.nom_serveur*`/custom`. Ensuite, dans le fichier de propriétés personnalisées de la boîte à outils, définissez la propriété `am.camtoolkit.gpe.customxml.custom` avec le nom (sans chemin d'accès) du fichier que vous avez modifié à l'étape 2, à la page 833.
   - Sauvegardez le fichier dans l'un des répertoires de votre ordinateur. Ensuite, dans le fichier de propriétés personnalisées de la boîte à outils, définissez la propriété `am.camtoolkit.gpe.customxml.custom` avec le nom et le chemin d'accès du fichier que vous avez modifié à l'étape 2, à la page 833.

   Pour plus d'informations sur le fichier de propriétés personnalisées du kit d'outils, voir «Fichier de propriétés du kit d'outils», à la page 817.

Activation d'un associateur de demande :

Pour activer un associateur de demande pour un type de demande, modifiez le fichier de configuration personnalisée du kit d'outils ou le fichier de configuration personnalisée globale du kit d'outils. Les procédures sont différentes pour les demandes communes et pour les demandes personnalisées.

Avant de commencer

Définissez la configuration de l'associateur de demande dans un fichier XML. Ensuite, placez ce fichier XML dans le même répertoire que le fichier de propriétés du kit d'outils.

- Pour activer l'associateur de demande pour toutes les instances du serveur d'applications, placez-le dans le répertoire *base_cd*/runtime/custom.
- Pour activer l'associateur de demande pour une instance du serveur d'applications, placez-le dans le répertoire *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/.

Pour plus d'informations sur la syntaxe du fichier XML, voir «Syntaxe du fichier XML», à la page 824.

Pourquoi et quand exécuter cette tâche

Editez le fichier toolkit_custom.properties ou le fichier toolkit_global_custom.properties pour activer l'associateur de demande pour une ou toutes les instances du serveur d'applications.

Procédure

- Pour activer un associateur de demande pour des demandes communes, procédez comme suit :
  1. Dans un éditeur de texte, ouvrez un des fichiers de configuration personnalisée suivants du kit d'outils :
     - Pour activer l'associateur de demande pour toutes les instances de serveur d'applications, ouvrez le fichier *base_cd*/runtime/custom/toolkit_global_custom.properties.
     - Pour activer l'associateur de demande pour une instance de serveur d'applications, ouvrez le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties.
  2. Editez le fichier de propriétés du kit d'outils comme suit :
     - Ajoutez une ligne définissant la propriété d'activation pour ce type de demande sur true. Pour plus d'informations, voir tableau 193, à la page 837.
     - Ajoutez une ligne définissant la propriété am.camtoolkit.gpe.customxml.* sur le nom du fichier XML de l'associateur. Utilisez des valeurs uniques au lieu du symbole "*". Pour plus d'informations, voir «Syntaxe du fichier XML», à la page 824.
  3. Sauvegardez et fermez le fichier de propriétés.

  Exemple :

  Pour activer un associateur de demande qui est défini dans renameDataSource.xml pour le type de demande SQL, ajoutez les lignes suivantes dans le fichier de configuration personnalisée du kit d'outils ou dans le fichier de configuration personnalisée globale du kit d'outils :

  ```
  com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
  am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
  ```

- Pour activer un associateur de demande pour des demandes personnalisées, effectuez les étapes suivantes :
  1. Sous la balise <edgerequest> dans le fichier XML de définition de demandes personnalisées, créez la balise >requestMapper<. Insérez un nom de type d'associateur de demande unique dans cette balise. Pour plus d'informations sur la définition des demandes personnalisées, voir «Définition de demandes personnalisées», à la page 833.
  2. Dans le fichier XML de l'associateur de demande, utilisez le nom unique de type d'associateur de demande dans l'attribut type de la balise >requestMapperDefinition<.
  3. Dans un éditeur de texte, ouvrez un des fichiers de configuration personnalisée suivants du kit d'outils :
     - Pour activer l'associateur de demande pour toutes les instances de serveur d'applications, ouvrez le fichier *base_cd*/runtime/custom/toolkit_global_custom.properties.

– Pour activer l'associateur de demande pour une instance de serveur d'applications, ouvrez le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties.

4. Editez le fichier de propriétés du kit d'outils pour ajouter une ligne définissant la propriété am.camtoolkit.gpe.customxml.* sur le nom du fichier XML de l'associateur. Utilisez des valeurs uniques au lieu du symbole "*". Pour plus d'informations, voir «Syntaxe du fichier XML», à la page 824.
5. Sauvegardez et fermez le fichier de propriétés.

Exemple :

Pour activer un associateur de demande qui est défini dans customMapper.xml pour le type de demande personnalisée SupplyCheck qui est défini dans le fichier custom_requests.xml, effectuez les étapes suivantes :

1. Utilisez la définition suivante dans le fichier custom_requests.xml :

```
<customEdgeRequests>
  <edgeRequest>
    <requestName>SupplyCheck</requestName>
    <Matches>com.mycompany.myapp.Supplier</Matches>
    <type>application</type
    <methodName>inventoryCheck</methodName>
    <requestMapper>customMapper</requestMapper>
  </edgeRequest>
</customEdgeRequests>
```

2. Dans le fichier customMapper.xml, assurez-vous que le nom du type est défini :

```
<requestMapperDefinition type="customMapper">
```

3. Ajoutez la ligne suivante dans le fichier de configuration personnalisée du kit d'outils ou dans le fichier de configuration personnalisée globale du kit d'outils :

```
am.camtoolkit.gpe.customxml.customMapper=customMapper.xml
```

Noms et données d'entrée et de sortie de l'associateur de demande :

Les tableaux suivants répertorient les informations nécessaires pour configurer et activer des associateurs de demande pour les différents types de demande.

La signification de chaque en-tête de tableau est expliquée comme suit :

Type de demande
Type de la demande.

Propriété d'activation
Pour activer l'associateur de demande, affectez à cette propriété la valeur true dans le fichier toolkit_custom.properties ou toolkit_global_custom.properties.

Important : Si vous copiez cette valeur depuis le tableau, supprimez les espaces et les retours à la ligne.

Nom de type d'associateur de demande
Affectez cette valeur à l'attribut type de la balise <requestMapperDefinition> dans le fichier XML de définition de l'associateur de demande.

Noms des symboles de données d'entrée
Symboles représentant les informations de demande. Vous pouvez utiliser ces symboles dans les expressions des définitions de l'associateur de demande. Pour plus d'informations, voir «Définition d'une expression», à la page 825.

Clés de contexte des données de sortie
Pour apporter des modifications aux informations de surveillance, vous pouvez attribuer des valeurs à ces clés dans la définition de l'associateur de demande. Pour plus d'informations, voir «Mappage de valeurs à des clés de contexte», à la page 831.

Tableau 193. Propriétés d'activation et noms de type de l'associateur de demande

Type de demande	Propriété d'activation	Nom de type d'associateur de demande
Servlet	com.ibm.tivoli.itcam.toolkit.ai.enable.servletrequestmapper	servlet
JNDI	com.ibm.tivoli.itcam.toolkit.ai.enable.jndirequestmapper	jndiLookup
Demande personnalisée		Définie par l'utilisateur dans la définition edgeRequest
EJB	com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper	ejb
JCA	com.ibm.tivoli.itcam.toolkit.ai.enable.jcarequestmapper	jca
Source de données JDBC	com.ibm.tivoli.itcam.toolkit.ai.enable.datasourcerequestmapper	dataSource
Instruction SQL JDBC	com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper	sqlStatement
JMS	com.ibm.tivoli.itcam.toolkit.ai.enable.jmsrequestmapper	jms
Service Web JAX-RPC	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
Service Web Axis	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
MQI	com.ibm.tivoli.itcam.toolkit.ai.enable.mqrequestmapper	mqi
EJB	com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper	ejb
Fabrique de connexions JDBC	com.ibm.tivoli.itcam.toolkit.ai.enable. sqlconnectfactoryrequestmapper	connectionFactory
SCA	com.ibm.tivoli.itcam.toolkit.ai.enable.scarequestmapper	sca
Service Web JAX-WS	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
WebSphere Portal Server (extension de la classe org.apache.jetspeed. portlet.Portlet)	com.ibm.tivoli.itcam.toolkit.ai.enable.portalrequestmapper	portalPortal
WebSphere Portal Server version 6.1, 7 et 8 (implémentation de l'interface javax.portlet.Portlet)	com.ibm.tivoli.itcam.toolkit.ai.enable.portal6requestmapper	Portal6Portal

Important : Il n'existe aucune manière significative de configurer l'associateur de demande personnalisé pour les types de requête qui ne sont pas répertoriés dans le tableau 193.

Tableau 194. Données d'entrée et de sortie de l'associateur de demande

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
Servlet	Pour plus d'informations, voir tableau 195, à la page 841.	**remappedURI** définit un identificateur URI renommé. **remappedURL** définit une adresse URL renommée. **appName** définit un nom d'application renommée. **userid** définit l'ID utilisateur associé à la demande.
JNDI	• **$jndiContext** objet contextuel • **$lookup** chaîne de recherche • **$context** "JNDIlookup"	**renamedLookup** définit une chaîne de recherche renommée.
Demande personnalisée	• **$this** objet 'this' associé à la méthode de la demande personnalisée • **$0** arguments communiqués à la méthode de la demande personnalisée, spécifiés sous la forme d'un tableau d'objets • **$className** nom de la classe de la demande personnalisée • **$methodName** nom de la méthode de la demande personnalisée • **$context** nom de la demande d'origine issu de la définition edgeRequest	**customRequestName** définit le nom de la demande personnalisée renommée
EJB	• **$ejb** objet de l'implémentation EJB • **$appName** nom de l'application • **$ejbType** type de l'EJB • **$className** nom de classe de l'objet d'implémentation EJB • **$methodName** nom de la méthode métier EJB • **$context** "EJBBusinessMethod"	**appName** définit le nom de l'application renommée **ejbType** définit le type EJB renommé **className** définit le nom de la classe renommée **methodName** définit le nom de la méthode renommée
JCA	• **$interaction** objet Interaction • **$interactionSpec** objet InteractionSpec • **$record** objet Record • **$context** "J2Cexecute"	**lookupName** est le nom de la recherche renommée **productName** est le nom du produit renommé **productVersion** est la version du produit renommé

Tableau 194. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
Source de données JDBC	• **$this** objet source de données ou objet pilote • **$dataSource** objet $this, transtypé en objet source de données • **$driver** objet $this, transtypé en objet pilote • **$dataSourceName** nom de la source de données, tel que java.lang.String • **$context** indique le type de demande "JDBCgetConnection" ou "JDBCgetConnection FromDriver"	**dataSourceName** est le nom de la source de données renommée, si l'objet $this est une source de données **url** est l'adresse URL du pilote renommé, si l'objet $this est un pilote
Instruction SQL JDBC	• **$this** instruction SQL ou connexion SQL • **$sqlText** contient le texte SQL sous la forme java.lang.String, si l'objet $this est une instruction SQL • **$sqlStatement** objet $this, transtypé en instruction SQL • **$sqlConnection** objet $this, transtypé en connexion SQL • **$dataSourceName** nom de la source de données • **$context** indique le type de demande : "JDBCexecute", JDBCexecuteQuery", "JDBCexecuteUpdate", "JDBCcreateStatement", "JDBCprepareStatement"	**dataSourceName** est le nom de la source de données renommée **sqlText** est le texte SQL renommé
JMS	• **$this** est l'objet ‘this' de la méthode instrumentée. Peut être QueueBrowser, MessageConsumer, MessageProducer ou MessageListener • **$0** objet de file d'attente pour une demande d'envoi, ou objet de rubrique pour une demande de publication • **$queueBrowser** objet $this, transtypé en objet de type QueueBrowser • **$messageConsumer** objet $this, transtypé en objet de type MessageConsumer • **$messageProducer** objet $this, transtypé en objet de type MessageProducer • **$messageListener** objet $this, transtypé en objet de type MessageListener • **$queue** objet $0, transtypé en file d'attente • **$topic** objet $0, transtypé en rubrique • **$context** indique le type de demande : "JMSreceive", "JMSsend", "JMSbrowse", "JMSpublish", "JMSonmessage"	**queueName** est le nom de la file d'attente renommée **providerURL** est l'URL du fournisseur renommé **topicName** est le nom de la rubrique renommée

Tableau 194. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
Service Web JAX-RPC	• **$messageContext** encapsuleur IMessageContextWrapper • **$appName** nom de l'application • **$requestName** nom de la demande par défaut • **$url** adresse URL • **$context** indique le type de demande : "WebServicesJaxRpc ProviderRequest", "WebServicesJaxRpc ClientRequest"	**appName** est le nom de l'application renommée **requestName** est le nom de la demande renommée **url** est l'adresse URL renommée
Service Web Axis	• **$messageContext** encapsuleur IMessageContextWrapper • **$appName** nom de l'application • **$requestName** nom de la demande par défaut • **$url** adresse URL • **$context** indique le type de demande : "WebServicesAxisClient Request", "WebServicesAxis ProviderRequest"	**appName** est le nom de l'application renommée **requestName** est le nom de la demande renommée **url** est l'adresse URL renommée
MQI	• **$queue** objet MQQueue, s'il est connu • **$qmgr** objet MQQueueManager, s'il est connu • **$message** objet MQMessage ou MQMsg2, s'il est connu • **$session** objet MQSESSION, s'il est connu • **$getMsgOptions** objet MQGetMessageOptions, s'il est connu • **$qmgrName** nom du gestionnaire de files d'attente • **$queueName** nom de la file d'attente • **$context** type de la demande MQ : "MQCONN", "MQCONNX", "MQDISC", "MQBACK", "MQBEGIN", "MQCLOSE", "MQCMIT", "MQINQ", "MQOPEN", "MQSET", "MQGET", "MQPUT", "MQPUT1", "MQGETBROWSE"	**qmgrName** est le nom du gestionnaire de files d'attente renommé **qname** est le nom de la file d'attente renommée
EJB	• **$appName** nom de l'application • **$ejbType** type de l'EJB • **$className** nom de classe de l'objet d'implémentation EJB • **$methodName** nom de la méthode métier EJB • **$context** "EJBBusinessMethod"	**appName** définit le nom de l'application renommée **ejbType** définit le type EJB renommé **className** définit le nom de la classe renommée **methodName** définit le nom de la méthode renommée

Tableau 194. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
Fabrique de connexions JDBC	• **$connectionFactory** fabrique de connexions • **$dataSourceName** nom de la source de données • **$context** "JDBCgetConnection"	**dataSourceName** est le nom de la source de données renommée
SCA	• **$uri** identificateur URI • **$operationName** nom d'opération • **$context** indique le type de demande : "SCA_Generic", "SCA_Ref", "SCA_Target"	**uri** est l'identificateur URI renommé **operationName** est le nom de l'opération renommée
Service Web JAX-WS	• **$messageContext** encapsuleur IMessageContextWrapper • **$appName** nom de l'application • **$requestName** nom de la demande par défaut • **$url** adresse URL • **$context** indique le type de demande : "WebServicesJAXWS ClientRequest", "WebServicesJAXWS ProviderRequest", "WebServicesJAXWS AsyncRequest"	**appName** est le nom de l'application renommée **requestName** est le nom de la demande renommée **url** est l'adresse URL renommée
WebSphere Portal Server (extension de la classe `org.apache.jetspeed.portlet.Portlet`)	• **$portletAdapter** PortletAdapter • **$portletRequest** PortletRequest • **$portletResponse** PortletResponse • **$portletName** nom du portlet • **$pageTitle** titre de la page • **$url** adresse URL de la demande • **$userid** ID utilisateur de la demande • **$context** "Portal.Portlet"	**portletName** est le nom du portlet renommé **title** est le titre de la page renommée **url** est l'adresse URL renommée **userid** est l'ID utilisateur renommé
WebSphere Portal Server version 6.1, 7 et 8 (implémentation de l'interface `javax.portlet.Portlet`)	• **$portlet** portlet • **$renderRequest** RenderRequest • **$renderResponse** RenderResponse • **$portletName** Nom du portlet • **$pageTitle** Titre de la page • **$url** Adresse URL de la demande • **$userid** ID utilisateur de la demande • **$context** "Portal.Portlet"	**portletName** Nom du portlet renommé **title** Titre de la page renommée **url** URL renommée **userid** ID utilisateur renommé

Pour les demandes de servlet, il existe un grand nombre de symboles de données d'entrée.

Tableau 195. Noms des symboles de données d'entrée disponibles pour les demandes de servlet

Nom du symbole	Type de valeur	Contenu du symbole
$context	String	"ServletMethod"
$servlet	javax.servlet.http.HttpServlet	Objet HttpServlet associé à la demande de servlet
$httpServletRequest	javax.servlet.http.HttpServletRequest	Objet HttpServletRequest associé à la demande de servlet

Tableau 195. Noms des symboles de données d'entrée disponibles pour les demandes de servlet (suite)

Nom du symbole	Type de valeur	Contenu du symbole
$httpServletResponse	javax.servlet.http.HttpServletResponse	Objet HttpServletResponse associé à la demande de servlet
$appName	java.lang.String	Nom d'application associé au servlet
$URL	java.lang.StringBuffer	Adresse URL que le client a utilisée pour faire la demande
$RemoteUser	java.lang.String	Nom de connexion de l'utilisateur qui effectue cette demande, s'il est authentifié
$URI	java.lang.String	Partie de l'URL de la demande allant du nom de protocole jusqu'à la chaîne de requête
$ServletPath	java.lang.String	Partie de l'URL de la demande qui appelle le servlet.
$SessionID	javax.servlet.http.HttpSession	Session en cours associée à la demande
$QueryString	java.lang.String	Chaîne de demande qui se trouve dans l'adresse URL de la demande, après le chemin.
$SessionAttribute	java.lang.String	Ce symbole paramétré retourne une valeur d'attribut de session. Il dispose d'un paramètre, le nom d'attribut (doit être une chaîne). Par exemple, `$SessionAttribute("attr1")` renvoie la valeur de l'attribut nommé attr1.
$cookie	javax.servlet.http.Cookie	Ce symbole paramétré retourne un cookie nommé. Il dispose d'un paramètre, le nom du cookie (doit être une chaîne). Par exemple, `$cookie("cookie1")` renvoie la valeur de l'attribut nommé cookie1.

Exemples de définition d'associateur de demande :

Les exemples suivants illustrent l'utilisation de l'associateur de demande.

Changement du nom d'application de servlet :

Dans cet exemple, le nom d'application figurant dans une demande de servlet est remplacé par l'URI et la chaîne de requête.

Le fichier *base_cd*`/runtime/changeAppname.xml` contient la définition d'associateur de demande suivante :

```
<gpe>
   <runtimeConfiguration>
         <requestMapperDefinition type="servlet">
               <selection>
                     <matchCriteria>true</matchCriteria>
                     <mapTo>
                           <key>appName</key>
                           <value>$URI + "." + $QueryString</value>
```

```
                    </mapTo>
                </selection>
            </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

Changement de nom d'une source de données :

Dans cet exemple, le nom de la source de données figurant dans une demande SQL est remplacé par un autre nom plus facile à comprendre.

Le fichier *base_cd*/runtime/renameDataSource.xml contient la définition suivante de l'associateur de demande :

```
<gpe>
 <runtimeConfiguration>
   <requestMapperDefinition type="sqlStatement">
      <selection>
         <matchCriteria>$dataSourceName != null</matchCriteria>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/TradeDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Daytrader Data Source"</value>
           </mapTo>
         </selection>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/LongDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Long term trader Data Source"</value>
           </mapTo>
         </selection>
      </selection>
   </requestMapperDefinition>
 </runtimeConfiguration>
<gpe>
```

La première balise <selection> garantit que $dataSourceName n'a pas la valeur null. Puis, la deuxième balise <selection> peut sans risque évaluer $dataSourceName.equals().

Si la première balise <selection> est absente et qu'une valeur null est transmise pour $dataSourceName, l'associateur de demande génère une exception. Dans ce cas, il manquera des données de surveillance dans le résultat de la demande.

Pour activer cet associateur de demande, le fichier *base_cd*/runtime/toolkit_global_custom.properties contient les lignes suivantes :

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Suppression des informations sensibles d'une demande SQL :

Dans cet exemple, une application inclut des numéros de sécurité sociale dans des demandes SQL. L'associateur de demande supprime les numéros de la version de la demande que l'utilisateur peut afficher.

Dans les demandes SQL, le numéro de sécurité sociale est répertorié avec le nom de colonne SS, SS = *numéro*. L'associateur de demande recherche la chaîne SS = et supprime les neuf symboles après cette chaîne.

Le fichier *base_cd*/runtime/removeSSN.xml contient la définition suivante de l'associateur de demande :

```
<gpe>
    <runtimeConfiguration>
         <requestMapperDefinition type="sqlStatement">
             <symbolDefinitions>
                 <symbol>
                     <name>$offsetOfSS</name>
                     <eval>$sqlText.indexOf("SS = ")</eval>
                 </symbol>
                 <symbol>
                     <name>$sqlTextContainsSS</name>
<eval>$sqlText != null AND $offsetOfSS > 0 AND $sqlText.length() GE
$offsetOfSS+16</eval>
                 </symbol>
                 <conditionalSymbol>
                     <name>$sqlTextPriorToSSKeyword</name>
                     <type>java.lang.String</type>
                     <defaultValue>""</defaultValue>
                     <if condition="$sqlTextContainsSS">
                       <return>$sqlText.substring(0, $offsetOfSS+5)</return>
                     </if>
                 </conditionalSymbol>
                 <conditionalSymbol>
                     <name>$sqlTextAfterSS</name>
                     <type>java.lang.String</type>
                     <defaultValue>""</defaultValue>
                     <if condition="$sqlTextContainsSS">
                       <return>$sqlText.substring($offsetOfSS+16)</return>
                     </if>
                 </conditionalSymbol>
             </symbolDefinitions>
             <selection>
                  <matchCriteria>$sqlText != null AND $sqlText.length() >
0</matchCriteria>
                  <selection>
                       <matchCriteria>$sqlTextContainsSS</matchCriteria>
                       <mapTo>
                            <key>sqlText</key>
                            <value>$sqlTextPriorToSSKeyword + "?" +
$sqlTextAfterSS</value>
                       </mapTo>
                  </selection>
             </selection>
         </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

Pour activer cet associateur de demande, le fichier *base_cd*/runtime/toolkit_global_custom.properties contient les lignes suivantes :

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=removeSSN.xml
```

Annulation de la configuration du collecteur de données pour les applications sur site

Si vous n'avez pas besoin de surveiller vos serveurs Liberty ou si vous souhaitez mettre à niveau le collecteur de données vers une nouvelle version, vous devez annuler la configuration du collecteur de données que vous avez déployé sur le serveur Liberty.

Pourquoi et quand exécuter cette tâche

Pour annuler la configuration du collecteur de données déployé sur le serveur Liberty, annulez les modifications apportées lors de la configuration du collecteur de données. Vous pouvez choisir de configurer le collecteur de données manuellement ou avec le script unconfig_liberty_dc fourni.

Procédure

- Pour annuler manuellement la configuration du collecteur de données, procédez comme suit :
  1. Accédez au répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
  2. Modifiez le fichier `jvm.options` pour supprimer les paramètres ci-dessous.

     ```
     -agentlib:am_ibm_16=nom_serveur
     -Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
     -Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
     -Dliberty.home=base_liberty
     -Xhealthcenter:level=inprocess
     -Xgc:allocationSamplingGranularity=10000
     -verbosegc
     -Xverbosegclog:chemin_accès_absolu_au_fichier_journal,1,10000
     ```
  3. Modifiez le fichier `server.env` dans le même répertoire pour supprimer la valeur suivante pour **`LD_LIBRARY_PATH`**

     `/lib:base_dc/toolkit/lib/lx8266:base_dc/toolkit/lib/lx8266/ttapi`

     où *base_dc* est le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.06`.
  4. Modifiez le fichier `server.xml` dans le même répertoire pour supprimer `<feature>monitor-1.0</feature>` de la section `<featureManager>`.
  5. Redémarrez le serveur Liberty.
- Pour annuler la configuration du collecteur de données avec le script `unconfig_liberty_dc.sh`, procédez comme suit :
  1. Accédez au répertoire *base_dc*`/bin`. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.06/bin`.
  2. Démarrez le script d'annulation de configuration en exécutant la commande suivante :

     `./unconfig_liberty_dc.sh`
  3. A l'invite de commande, entrez la racine de votre répertoire d'installation Liberty ou acceptez la valeur par défaut. Par exemple, `/opt/ibm/wlp`.
  4. Le programme d'annulation de configuration peut reconnaître et répertorier automatiquement les serveurs d'applications configurés dans le répertoire spécifié. Entrez le numéro qui correspond au serveur Liberty dont vous souhaitez annuler la configuration. Pour sélectionner plusieurs serveurs, séparez les numéros par un espace ou entrez `*` pour sélectionner tous les serveurs.
  5. Une fois que le programme d'annulation de configuration a fini de mettre à jour les fichiers de tous les serveurs Liberty, redémarrez les serveurs pour que les modifications soient prises en compte.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Vous pouvez également supprimer le répertoire de base du collecteur de données si vous n'en avez plus besoin.

Configuration du collecteur de données Liberty pour les applications IBM Cloud

Pour surveiller un profil Liberty exécuté dans l'environnement IBM Cloud, vous devez télécharger le package du collecteur de données à partir d'IBM Passport Advantage, déployer le collecteur de données dans vos fichiers d'application locaux, puis envoyer les mises à jour par push à IBM Cloud.

Avant de commencer

Il est supposé que l'application Liberty est envoyée par push à l'environnement IBM Cloud avec les commandes Cloud Foundry. Le fichier `manifest.yml` et le répertoire de base Liberty (qui contient le fichier `server.xml`) existe déjà.

Si votre application Liberty est déployée sous forme de fichier WAR, vous devez modifier certains fichiers locaux de façon à mettre à jour l'application en envoyant un répertoire local contenant le fichier WAR et les fichiers de collecteur de données. Un exemple expliquant comment obtenir un répertoire principal de serveur Liberty local lorsque vous disposez uniquement du fichier WAR est fourni ici.

1. Exécutez la commande suivante pour exécuter l'application Liberty en local :

   ```
   mvn install liberty:run-server
   ```

   Dans le répertoire qui contient le fichier WAR Liberty, un sous-répertoire `/liberty/wlp/usr/servers/defaultServer` est créé. Ce répertoire peut servir de répertoire principal de serveur Liberty dans la procédure suivante.
2. Dans le répertoire racine qui contient le fichier WAR Liberty, copiez le dossier entier *nom_application*`-SNAPSHOT` dans le répertoire `/liberty/wlp/usr/servers/defaultServer`.
3. Dans le répertoire `/liberty/wlp/usr/servers/defaultServer`, éditez le fichier `bootstrap.properties` de façon à modifier le chemin **appLocation**. Le chemin **appLocation** doit être défini sur le chemin relatif du répertoire de l'application dans IBM Cloud.
4. Supprimez les dossiers `logs` et `workarea`. Ils n'ont pas besoin d'être envoyés par push à IBM Cloud.
5. Modifiez la valeur de **path** dans le fichier `manifest.yml` de façon à ce qu'elle pointe vers le répertoire `defaultServer`.

   Par exemple, `path: target/liberty/wlp/usr/servers/defaultServer`.

Procédure

Pour configurer le collecteur de données Liberty, procédez comme suit :

1. Téléchargez le module du collecteur de données `_datacollectors_linux_8.1.4.0.5.tgz` à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
2. Configurez le package du collecteur de données avec les scripts `make_configuration_packages.sh` et `configure_agent_images.sh` sur le système sur lequel le serveur Cloud APM est installé. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.
3. Exécutez la commande suivante pour extraire les fichiers du package de collecteur de données :

   ```
   tar -xzf _datacollectors_linux_8.1.4.0.5.tgz
   ```

   Le module `liberty_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
4. Extrayez les fichiers à partir du module `liberty_datacollector_8.1.4.0.tgz` dans un répertoire temporaire.

   ```
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Par exemple,

   ```
   cd /root/tmp
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Vous pouvez rechercher les fichiers extraits dans le répertoire `liberty_dc` dans le répertoire temporaire.
5. Copiez le répertoire `.gdc` du répertoire `liberty_dc` dans le répertoire de base de votre serveur Liberty sur lequel le fichier `server.xml` est stocké. Le répertoire de base du serveur Liberty est appelé *rép_principal_serveur_liberty* dans les étapes ci-après.

   ```
   cp -rf rép_temp/liberty_dc/.gdc rép_principal_serveur_liberty
   ```

Par exemple,

```
cp -rf /root/tmp/liberty_dc/.gdc /opt/liberty855/wlp/usr/servers/defaultServer/
```

6. Copiez ou fusionnez le contenu des fichiers `jvm.options` et `server.env` du répertoire `liberty_dc/etc` dans le répertoire *rép_principal_serveur_liberty*.
   - Si les fichiers `jvm.options` et `server.env` ne se trouvent pas dans le répertoire *rép_principal_serveur_liberty*, copiez-les de *rép_temp*`/liberty_dc/etc` dans *rép_principal_serveur_liberty*.

     ```
     cp rép_temp/liberty_dc/etc/jvm.option rép_principal_serveur_liberty
     cp rép_temp/liberty_dc/etc/server.env rép_principal_serveur_liberty
     ```

   - Si le fichier `jvm.options` ou `server.env` existe dans le répertoire *rép_principal_serveur_liberty*, fusionnez son contenu avec les fichiers du répertoire *rép_temp*`/liberty_dc/etc`.
7. Si vos applications IBM Cloud ne peuvent pas se connecter directement au serveur Cloud APM en raison des paramètres de réseau ou de pare-feu, configurez le collecteur de données pour l'envoi du trafic par le biais d'un proxy direct. Pour cela, modifiez le fichier `jvm.options` de l'une des manières suivantes :
   - Si l'authentification n'est pas requise, ajoutez les lignes suivantes au fichier :

     ```
     -Dhttp.proxyHost=hôte_proxy_http
     -Dhttp.proxyPort=port_proxy_http
     -Dhttps.proxyHost=hôte_proxy_http
     -Dhttps.proxyPort=port_proxy_http
     -Djava.net.useSystemProxies=true
     ```

   - Si un nom d'utilisateur et un mot de passe sont requis pour accéder au serveur proxy direct, ajoutez les lignes suivantes au fichier :

     ```
     -Dhttp.proxyHost=hôte_proxy_http
     -Dhttp.proxyPort=port_proxy_http
     -Dhttp.proxyUser=utilisateur_proxy_http
     -Dhttp.proxyPassword=mot_de_passe_proxy_http
     -Dhttps.proxyHost=hôte_proxy_http
     -Dhttps.proxyPort=port_proxy_http
     -Dhttps.proxyUser=utilisateur_proxy_http
     -Dhttps.proxyPassword=mot_de_passe_proxy_http
     -Djava.net.useSystemProxies=true
     ```

8. Modifiez le fichier `server.xml` dans le répertoire de base du serveur Liberty pour activer la fonction de surveillance en ajoutant la ligne suivante à la section `<featureManager>` :

   ```
   <featureManager>
                <feature>monitor-1.0</feature>
   </featureManager>
   ```

9. Modifiez le fichier `manifest.yml` de votre application Liberty pour allouer 512 Mo de mémoire supplémentaire.
10. Ouvrez une invite de commande et accédez au répertoire local qui contient le fichier `manifest.yml` pour le serveur Liberty. Par exemple, `/opt/liberty855/`.
11. Connectez-vous à IBM Cloud et mettez à jour le profil Liberty avec la commande **`cf push`**.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM. La surveillance des ressources, le suivi des transactions et les données de diagnostic sont activées. Toutefois, la collecte de segments de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez les activer avec les fichiers de propriétés du collecteur de données si vous avez besoin des données contenues dans les tableaux de bord Cliché de tas et Analyse de mémoire.

Que faire ensuite

- Si vous êtes un utilisateur public de IBM Cloud, configurez la passerelle sécurisée IBM Cloud pour lui permettre de se connecter au serveur Cloud APM. Pour plus d'informations, voir «Configuration de la passerelle sécurisée IBM Cloud», à la page 234.

- Pour afficher les données de surveillance de votre application IBM Cloud, démarrez la console Cloud APM. Pour les instructions, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

  A faire : Si vous souhaitez ajouter l'instance de collecteur de données Liberty sur le Tableau de bord des applications, sélectionnez **Liberty Runtime** au lieu de **WebSphere Application Server** dans la liste des composants.
- Pour que les tableaux de bord Cliché de tas et/ou Analyse de mémoire contiennent des données, vous devez également activer la collecte des données pour le collecteur d'instantané de segment de mémoire et/ou la collecte d'allocation de mémoire, ce qui est faisable dans les fichiers `.properties` du collecteur de données. Voir «Personnalisation du collecteur de données avec des fichiers de propriétés», à la page 850.
- Si le fichier de clés ou le serveur Cloud APM est modifié, reconnectez le collecteur de données au serveur Cloud APM. Pour plus d'informations, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 234.

Variables d'environnement pour la personnalisation du collecteur de données Liberty

Pour personnaliser le collecteur de données Liberty pour les applications IBM Cloud, utilisez l'interface utilisateur IBM Cloud pour ajouter les variables d'environnement prises en charge par le collecteur de données.

Conseil : Pour ajouter des variables d'environnement dans l'interface utilisateur IBM Cloud, connectez-vous d'abord à l'interface utilisateur IBM Cloud, puis cliquez sur votre application et sur **Exécution** > **Variable d'environnement**. Dans la section **définie par l'utilisateur**, ajoutez les variables d'environnement.

- Utilisez les variables répertoriées dans la rubrique tableau 196 pour configurer la connexion entre le collecteur de données Liberty et le serveur Cloud APM.
- Utilisez la variable répertoriée dans tableau 197, à la page 849 pour activer ou désactiver la trace de méthode pour vos applications IBM Cloud.
- Après avoir activé la méthode de traçage, utilisez les variables répertoriées dans tableau 198, à la page 849 pour indiquer des seuils pour les différents types de demande, afin que des niveaux différents de données de surveillance puissent être collectés.

A faire : Après avoir ajouté ou modifié la variable d'environnement, redémarrez votre application pour que les modifications soient prises en compte.

Tableau 196. Variables d'environnement pour les connexions serveur

Nom de la variable	Valeurs admises	Description
APM_BM_GATEWAY_URL	• `https://` *`IP_ou_nom_d'hôte_du_serveur`*`:443` • `http://` *`IP_ou_nom_d'hôte_du_serveur`*`:80`	URL de la passerelle du serveur Cloud APM cible.
APM_KEYFILE_PSWD	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n` *`<mot de passe du fichier de clés>`* `| base64` pour chiffrer votre mot de passe. **A faire :** Définissez cette variable uniquement lorsque vous avez configuré la variable *APM_BM_GATEWAY_URL* pour utiliser HTTPS.

Tableau 196. Variables d'environnement pour les connexions serveur (suite)

Nom de la variable	Valeurs admises	Description
APM_KEYFILE_URL	`http://serveur_http_hébergé:port/keyfile.jks`	L'URL de téléchargement du fichier de clés. **A faire :** Définissez cette variable uniquement lorsque vous avez configuré la variable *APM_BM_GATEWAY_URL* pour utiliser HTTPS.

Tableau 197. Variable d'environnement pour la trace de méthode

Nom de la variable	Valeurs admises	Description
METHOD_TRACE_ENABLE	• `true` • `false`	Cette variable permet d'activer ou de désactiver la méthode de traçage. La valeur `true` active cette fonction. La valeur par défaut est `false`.

Une fois que la trace de méthode a été activée, vous pouvez configurer des seuils pour les différents types de demande de façon à personnaliser la trace de méthode. Les méthodes suivantes, qui déclenchent la collecte de différents niveaux de données de surveillance, peuvent être configurées pour chaque type de demande :

Seuils principaux
Si vous configurez le seuil principal pour un type de demande, les informations temporelles de ce type de demande, telles que le temps UC et le temps de réponse, sont capturées. Par conséquent, si l'exécution d'une demande prend plus de temps que la durée spécifiée pour le seuil principal, le temps de la demande est capturé.

Seuils secondaires
Si vous configurez le seuil secondaire pour un type de demande, des données contextuelles approfondies sont capturées, par exemple les traces de pile et le code SQL pour les requêtes de base de données. Les données contextuelles capturées varient en fonction du type de demande. Si l'exécution d'une demande prend plus de temps que la valeur de seuil indiquée pour le seuil secondaire, ses données contextuelles sont capturées.

La variable d'environnement des différents seuils de demande est nommée *<type_demande>_<niveau seuil>*. Par exemple, pour configurer un seuil principal pour la demande JMS, ajoutez la variable `JMS_PRIMARY` et définissez sa valeur.

Le tableau 198 répertorie les variables d'environnement correspondantes que vous pouvez ajouter pour les différents types de demande. Les valeurs sont exprimées en millisecondes.

Tableau 198. Variables d'environnement pour les différents seuils de demande

Nom de la variable	Valeur par défaut (en millisecondes)
SERVLET_PRIMARY	20
SERVLET_SECONDARY	50
JDBC_PRIMARY	20
JDBC_SECONDARY	50
JNDI_PRIMARY	20
JNDI_SECONDARY	50
EJB_PRIMARY	20
EJB_SECONDARY	50

Tableau 198. Variables d'environnement pour les différents seuils de demande (suite)

Nom de la variable	Valeur par défaut (en millisecondes)
WEBSERVICES_PRIMARY	20
WEBSERVICES_SECONDARY	50
APP_METHODS_PRIMARY (méthodes d'application – non J2EE)	50
APP_METHODS _SECONDARY	1000
JCA_PRIMARY	50
JCA_SECONDARY	80
JMS_PRIMARY	40
JMS_SECONDARY	70

Personnalisation du collecteur de données avec des fichiers de propriétés

Par défaut, le suivi des transactions et des méthodes est activé pour le collecteur de données. La collecte des instantanés de segment de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez personnaliser la collecte de données ou les intervalles auxquels les données de diagnostic sont collées en modifiant les fichiers `.properties` du collecteur de données.

Pourquoi et quand exécuter cette tâche

Les fichiers de propriétés du collecteur de données sont dans le répertoire *base_dc*, par exemple `/opt/liberty855/wlp/usr/servers/defaultServer/.gdc/7.3.0.14.06`. Utilisez les différents fichiers de propriétés pour personnaliser le collecteur de données pour atteindre les objectifs suivants :

- Activation ou désactivation du suivi des transactions.
- Activation ou désactivation de la collecte d'instantanés de segment de mémoire.
- Spécification de l'intervalle auquel le collecteur de données prend un instantané du cliché de tas.
- Activation ou désactivation de la surveillance de l'allocation de mémoire.
- Spécification de l'intervalle auquel le collecteur de données collecte les informations d'allocation de mémoire.
- Activation ou désactivation du suivi des méthodes.

A faire : Après avoir modifié les fichiers `.properties`, utilisez la commande **`cf push`** pour envoyer les mises à jour par push à l'environnement IBM Cloud.

Procédure

- Pour activer ou désactiver le suivi des transactions, définissez la propriété **`com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled`** dans le fichier suivant sur `true` ou `false` :

  base_dc`/ldc/etc/ldc.properties` Si le suivi des transactions est activé, vous pouvez surveiller la pile d'application IBM Java dans les topologies.
- Pour activer ou désactiver la collecte des instantanés de segment de mémoire, définissez les propriétés **`com.ibm.tivoli.itcam.hc.send.heap.enable`** et **`com.ibm.tivoli.itcam.hc.snapshot.automatic.enable`** dans le fichier suivant sur `true` ou `false`.

  base_dc`/healthcenter/etc/hc.properties` Si la collecte d'instantanés de segment de mémoire est activée, le collecteur de données peut prendre un instantané de segment de mémoire à intervalles spécifiés. Les informations sur le cliché de tas peuvent être affichées dans le tableau de bord Cliché de tas.

- Pour modifier l'intervalle auquel l'instantané de segment de mémoire est pris par le collecteur de données, définissez la propriété **com.ibm.tivoli.itcam.hc.snapshot.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est 360.

  base_dc/healthcenter/etc/hc.properties
- Pour activer ou désactiver la collecte d'allocation de mémoire, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** dans le fichier suivant sur true ou false.

  base_dc/healthcenter/etc/hc.properties

  A faire : Pour activer la collecte d'allocation de mémoire, assurez-vous également que les deux lignes suivantes sont ajoutées au fichier jvm.options du serveur Liberty.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

  Une fois que la collecte d'allocation de mémoire est activée, les données sont disponibles dans le tableau de bord Analyse de la mémoire.
- Pour spécifier l'intervalle auquel les informations d'allocation de mémoire sont collectées, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est 15.

  base_dc/healthcenter/etc/hc.properties
- Pour activer ou désactiver le suivi des méthodes, définissez la propriété **dfe.enable.methoddata** dans le fichier suivant sur true ou false:

  base_dc/gdc/etc/gdc_dfe.properties

Que faire ensuite

- Une fois que le suivi des méthodes est activé, vous pouvez définir des seuils pour différents types de demande à l'aide des variables d'environnement, afin que des niveaux différents de données de surveillance puissent être collectés pour des demandes différentes. Pour les variables d'environnement applicables, voir tableau 198, à la page 849.
- Si vous avez désactivé la collecte d'allocation de mémoire, n'oubliez pas de supprimer les lignes suivantes du fichier jvm.options du serveur Liberty :

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

Annulation de la configuration du collecteur de données pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller vos profils Liberty dans l'environnement IBM Cloud ou si vous souhaitez mettre à niveau le collecteur de données vers une nouvelle version, vous devez annuler la configuration du collecteur de données que vous avez précédemment déployé.

Pourquoi et quand exécuter cette tâche

Pour annuler la configuration du collecteur de données pour votre profil Liberty dans l'environnement IBM Cloud, annulez les modifications apportées aux fichiers jvm.options, server.env et server.xml, puis mettez à jour le profil Liberty dans IBM Cloud avec la commande **cf push**.

Procédure

1. Dans votre répertoire local du profil Liberty, modifiez le fichier jvm.options pour supprimer les paramètres suivants. Vous pouvez supprimer le fichier s'il est vide après la modification.

   ```
   -agentlib:am_ibm_16=defaultServer
   -Xbootclasspath/p:../../../../.gdc/7.3.0.14.06/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=../../../../.gdc/7.3.0.14.06/itcamdc/etc/datacollector
   .policy
   -Dliberty.home=/home/vcap/app/.liberty
   ```

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:/home/vcap/app/wlp/usr/servers/defaultServer/logs/gc.log,1,10000
```

2. Dans le fichier `server.env`, supprimez la valeur suivante pour la variable d'environnement **`LD_LIBRARY_PATH`**. Vous pouvez supprimer le fichier s'il est vide après la modification.

```
LD_LIBRARY_PATH=:/lib:../../../../.gdc/7.3.0.14.06/toolkit/lib/lx8266
:../../../../.gdc/7.3.0.14.06/toolkit/lib/lx8266/ttapi
```

3. Modifiez le fichier `server.xml` pour supprimer la fonction monitor-1.0 en retirant la ligne suivante de la section `<featureManager>`

```
<feature>monitor-1.0</feature>
```

4. Supprimez la répertoire `.gdc` dans le répertoire de base Liberty.
5. Ouvrez une invite de commande, accédez au répertoire qui contient le fichier `manifest.yml` du serveur Liberty.
6. Connectez-vous à IBM Cloud et mettez à jour le profil Liberty avec la commande **`cf push`**.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 237.

Configuration de la surveillance de WebSphere Infrastructure Manager

Configurez l'Agent WebSphere Infrastructure Manager pour surveiller les performances de WebSphere Deployment Manager et de l'agent de noeud.

Pourquoi et quand exécuter cette tâche

L'Agent WebSphere Infrastructure Manager est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Procédure

1. Pour configurer l'agent, exécutez la commande ci-après.

```
rép_install/bin/wim-agent.sh config nom_instance
```

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent WebSphere Infrastructure Manager. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
2. A l'invite `Edit 'Monitoring Agent for WebSphere Infrastructure Manager' settings`, entrez `1` pour continuer.
3. A l'invite `Java home`, spécifiez le répertoire dans lequel Java est installé. La valeur par défaut est `/opt/ibm/apm/agent/JRE/lx8266/jre`.
4. A l'invite `DMGR Profile Home`, spécifiez le répertoire de base du profil Deployment Manager. Le répertoire par défaut est `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01`.
5. A l'invite `JMX user ID`, spécifiez l'ID utilisateur utilisé pour se connecter au serveur MBean.
6. A l'invite `Enter JMX password`, spécifiez le mot de passe de l'utilisateur.
7. A l'invite `Re-type JMX password`, entrez une nouvelle fois le mot de passe.
8. Pour démarrer l'agent, exécutez la commande ci-après.

```
rép_install/bin/wim-agent.sh start nom_instance
```

Résultats

Vous avez créé une instance Agent WebSphere Infrastructure Manager et démarré l'agent de surveillance pour commencer la collecte des échantillons de données pour la surveillance des données.

Configuration de la surveillance de WebSphere MQ

Pour pouvoir démarrer l'agent, vous devez d'abord lui affecter un nom d'instance et effectuer plusieurs tâches de configuration relatives à l'ID utilisateur et aux noms de système géré. De plus, vous pouvez éventuellement activer le suivi des transactions pour l'agent.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau tableau 199.

Tableau 199. Versions d'agent

Version d'agent	Documentation
7.3.0.7, 7.3.0.8, 7.3.0.9, 7.3.0.10, 7.3.0.11	Cloud APM 8.1.4
7.3.0.4	IBM Performance Management 8.1.3
7.3.0.3	IBM Performance Management 8.1.2
7.3.0.2	IBM Performance Management 8.1.1

- Assurez-vous que votre environnement possède la configuration système requise pour l'Agent WebSphere MQ. Pour les toutes dernières informations sur la configuration système requise, voir le rapport détaillé sur la configuration système requise pour l'Agent WebSphere MQ.

Pourquoi et quand exécuter cette tâche

Pour configurer l'environnement pour l'Agent WebSphere MQ, vous devez commencer par vérifier que l'ID utilisateur de l'agent peut accéder aux objets IBM MQ (WebSphere MQ), configurer IBM MQ (WebSphere MQ) pour l'activation des données, puis configurer l'Agent WebSphere MQ.

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'Agent WebSphere MQ. Effectuez les étapes nécessaires en fonction de vos besoins.

Procédure

1. Autorisez l'ID utilisateur qui est employé pour configurer, démarrer et arrêter l'agent à accéder aux objets IBM MQ (WebSphere MQ). Voir «ID utilisateur autorisés à exécuter l'agent», à la page 854.
2. Configurez IBM MQ (WebSphere MQ) pour activer les données que vous voulez surveiller. Voir «Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données», à la page 855.
3. Configurez l'agent en fournissant un nom d'instance d'agent, un nom de gestionnaire de files d'attente et, éventuellement, un nom d'agent. Voir «Configuration de l'Agent WebSphere MQ», à la page 857.
4. Facultatif : En fonction de vos exigences en termes de surveillance, vous pourriez avoir besoin d'un nom de système géré unique pour distinguer les agents de surveillance. Utilisez l'option `Agent Name` dans la commande `mq-agent.sh config` pour spécifier le qualificatif intermédiaire du nom de système géré. Voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 860.
5. Facultatif : Pour configurer l'agent en vue de collecter les données de suivi des transactions du gestionnaire de files d'attente surveillées, utilisez la page Configuration d'agent. Pour plus d'informations, voir «Configuration du suivi des transactions pour l'Agent WebSphere MQ», à la page 862.

6. Facultatif : Autorisez l'agent à collecter les données d'historique à long terme pour les files d'attente et les canaux. Pour obtenir des instructions, voir «Activation de la collecte de données pour l'historique à long terme de files d'attente et de canal», à la page 863.
7. Facultatif : Pour surveiller le gestionnaire de files d'attente à distance sur MQ Appliance, vous devez effectuez des étapes de configuration supplémentaires sur l'agent et IBM MQ (WebSphere MQ). Pour plus d'informations, voir «Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance», à la page 864 ou «Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance», à la page 866.

ID utilisateur autorisés à exécuter l'agent

Pour qu'un ID utilisateur puisse configurer, démarrer et arrêter l'Agent WebSphere MQ, il doit appartenir au groupe **mqm**, qui dispose de privilèges d'administration complets sur IBM MQ (WebSphere MQ). En outre, pour un utilisateur non superutilisateur ou un utilisateur non administrateur, vous devez accorder aux utilisateurs l'accès aux objets IBM MQ (WebSphere MQ) à l'aide de la commande de contrôle IBM MQ (WebSphere MQ).

Pourquoi et quand exécuter cette tâche

Sur AIX ou Linux, vous devez ajouter l'ID utilisateur au groupe **mqm** et puis accorder à l'ID utilisateur l'accès approprié aux objets IBM MQ (WebSphere MQ) avec la commande **setmqaut**.

Sur les systèmes Windows, vous devez ajouter l'identificateur utilisateur au groupe **mqm**. Si l'ID utilisateur ne fait pas partie du groupe d'utilisateurs Administrateur, vous devez également utiliser l'éditeur de registre pour accorder à l'ID utilisateur des autorisations lui permettant de démarrer ou d'arrêter l'agent.

Procédure

- Linux AIX Sur un système AIX ou Linux, procédez comme suit :
  1. Connectez-vous au système AIX ou Linux en utilisant l'ID racine.
  2. Ajoutez l'ID utilisateur qui est utilisé pour exécuter l'agent sur le groupe **mqm**.
  3. (WebSphere MQ version 7.5 ou ultérieure) : si l'ID utilisateur n'est pas celui d'un superutilisateur sur le système AIX ou Linux, vous devez lui accorder le niveau de droit approprié pour accéder aux objets IBM MQ (WebSphere MQ) en exécutant la commande suivante :

     ```
     setmqaut -m gestionnaire_files_attente -t qmgr -p ID_utilisateur +inq +connect +dsp +setid
     ```

     où *gestionnaire_files_attente* est le nom du gestionnaire de files d'attente de WebSphere MQ version 7.5 ou ultérieure et *ID_utilisateur* l'ID d'un utilisateur non superutilisateur ou non administrateur pour exécuter l'agent.
- Windows Sur les systèmes Windows, procédez comme suit :
  1. Connectez-vous aux systèmes Windows comme administrateur système.
  2. Ajoutez l'ID utilisateur qui est utilisé pour exécuter l'agent sur le groupe **mqm**.
  3. Si l'ID utilisateur que vous utilisez pour démarrer, exécuter et arrêter l'agent n'est pas membre du groupe Administrateur, utilisez l'éditeur de registre pour définir les droits d'un ID utilisateur afin de garantir que l'agent peut être démarré et arrêté correctement :
     a. Cliquez sur **Démarrer** > **Exécuter**, puis tapez `regedit.exe` pour ouvrir l'éditeur de registre.
     b. Dans l'éditeur de registre, recherchez la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.
     c. Cliquez avec le bouton droit sur la clé et cliquez sur **Autorisations**.
     d. Si l'ID utilisateur pour l'Agent WebSphere MQ n'est pas dans la liste Groupe ou noms d'utilisateur, cliquez sur **Ajouter** pour ajouter cet ID utilisateur à la liste.
     e. Cliquez sur l'ID utilisateur dans la liste.

f. Dans la liste des autorisations pour l'*ID_utilisateur*, où *ID_utilisateur* est l'ID utilisateur de l'Agent WebSphere MQ, sélectionnez **Contrôle total** dans la colonne Autoriser, puis cliquez sur **OK**.

g. Dans l'éditeur de registre, recherchez la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.

h. Cliquez avec le bouton droit sur la clé et cliquez sur **Autorisations**.

i. Si l'ID utilisateur pour l'Agent WebSphere MQ n'est pas dans la liste Groupe ou noms d'utilisateur, cliquez sur **Ajouter** pour ajouter cet ID utilisateur à la liste.

j. Cliquez sur l'ID utilisateur dans la liste Groupe ou noms d'utilisateur.

k. Dans la liste des autorisations pour l'*ID_utilisateur*, où *ID_utilisateur* est l'ID utilisateur de l'Agent WebSphere MQ, sélectionnez **Lecture** dans la colonne Autoriser, puis cliquez sur **OK**.

l. Fermez l'éditeur de registre.

m. Accédez au répertoire *rép_install*, où *rép_install* est le répertoire d'installation de l'agent.

n. Cliquez avec le bouton droit et cliquez sur **Propriétés**.

o. Sous l'onglet Sécurité, si l'ID utilisateur pour l'Agent WebSphere MQ n'est pas dans la liste Groupe ou noms d'utilisateur, cliquez sur **Editer**, puis sur **Ajouter** pour ajouter cet ID utilisateur à la liste.

p. Cliquez sur l'ID utilisateur dans la liste Groupe ou noms d'utilisateur.

q. Dans la liste des autorisations pour l'*ID-utilisateur*, sélectionnez **Contrôle total** dans la colonne Autoriser, où **ID-utilisateur** est l'ID utilisateur de l'Agent WebSphere MQ.

r. Cliquez sur **OK**.

Que faire ensuite

L'étape suivante consiste à configurer IBM MQ (WebSphere MQ) pour l'activation des données. Voir «Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données».

Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données

Avant de configurer l'Agent WebSphere MQ, il est recommandé de commencer par configurer IBM MQ (WebSphere MQ) pour activer les données que vous voulez surveiller.

Pourquoi et quand exécuter cette tâche

Déterminez le type de données que vous voulez surveiller à l'aide de l'Agent WebSphere MQ. Activez les données au niveau du gestionnaire de files d'attente en utilisant les commandes MQSC si les données ne sont pas générées par le gestionnaire de files d'attente par défaut.

A faire : Vous devez démarrer MQSC pour le gestionnaire de files d'attente cibles cible avant d'exécuter les commandes MQSC. Pour obtenir la liste des gestionnaires de files d'attente, exécutez la commande **dspmq** à partir du répertoire `bin` dans le répertoire d'installation d'IBM MQ (WebSphere MQ). Pour démarrer MQSC pour un gestionnaire de files d'attente, exécutez la commande suivante à partir du répertoire `bin`, où <*nom_gest_files_att*> correspond au nom du gestionnaire de files d'attente que vous voulez configurer.

```
runmqsc <nom_gest_files_att>
```

Procédure

- Pour voir l'ancienneté du message le plus ancien d'une file d'attente, effectuez les étapes expliquées dans la rubrique «Activation de la surveillance en temps réel des files d'attente», à la page 856.
- Pour surveiller les événements du gestionnaire de files d'attente qui ne sont pas générés par le gestionnaire de files d'attente par défaut, procédez comme décrit à la rubrique «Activation de la surveillance des événements pour le gestionnaire de files d'attente», à la page 856.

- Pour obtenir les données de suivi des transactions, procédez comme décrit à la rubrique «Activation de la trace de l'activité des applications MQI», à la page 857.
- Pour surveiller un gestionnaire de files d'attente éloignées, vérifiez que l'Agent WebSphere MQ peut collecter les données de surveillance par l'intermédiaire d'un canal du système distant. Pour plus d'informations, voir «Paramètres de sécurité de la surveillance éloignée», à la page 857.

Activation de la surveillance en temps réel des files d'attente

Pourquoi et quand exécuter cette tâche

Pour voir l'ancienneté du message le plus ancien d'une file d'attente (en secondes), vous devez activer la surveillance en temps réel de la file d'attente.

Procédure

Pour activer la surveillance en temps réel des files d'attente de votre environnement, utilisez les commandes ci-après.

- Pour activer la surveillance en temps réel de toutes les files d'attente dont l'attribut MONQ est défini sur QMGR, exécutez la commande suivante :

  ```
  ALTER QMGR MONQ(niveau_collecte)
  ```

  , *niveau_collecte* spécifiant le niveau de collecte des données de surveillance pour les files d'attente. Vous pouvez définir ce niveau sur LOW, MEDIUM ou HIGH selon les besoins de votre environnement.
- Pour activer la surveillance en temps réel d'une file d'attente individuelle, exécutez la commande suivante :

  ```
  ALTER QLOCAL(nom_file) MONQ(niveau_collecte)
  ```

  où *nom_file* représentant le nom de la file d'attente et *niveau_collecte*, le niveau de collecte des données de surveillance pour les files d'attente. Vous pouvez définir ce niveau sur LOW, MEDIUM ou HIGH selon les besoins de votre environnement.

Résultats

Les données peuvent être affichées dans le widget de groupe Ancienneté du plus ancien message de la file d'attente après le démarrage de l'Agent WebSphere MQ.

Activation de la surveillance des événements pour le gestionnaire de files d'attente

Pourquoi et quand exécuter cette tâche

La surveillance des événements fait partie des techniques de surveillance disponibles pour surveiller votre réseau IBM MQ. Après avoir activé le gestionnaire de files d'attente afin d'émettre certains types d'événement, des messages d'événement sont mis en file d'attente d'événements lorsque l'événement se produit, de sorte à pouvoir être surveillés et affichés par l'Agent WebSphere MQ.

Les types d'événement suivants ne sont ni surveillés ni affichés avec la configuration du gestionnaire de files d'attente par défaut. Utilisez la commande **ALTER QMGR** pour permettre au gestionnaire de files d'attente de générer ces événements afin qu'ils puissent être affichés sur le Tableau de bord d'Application Performance.

- Evénements de canal
- Evénements de performance

Procédure

Utilisez les commandes suivantes pour permettre au gestionnaire de files d'attente de générer les événements qui vous intéressent :

- Pour générer des événements de canal, exécutez `ALTER QMGR CHLEV(ENABLED)`.
- Pour générer des événements de performance, exécutez `ALTER QMGR PERFMEV(ENABLED)`.

Résultats

Les événements surveillés peuvent être affichés dans le widget de groupe Evénements du gestionnaire de files d'attente une fois l'Agent WebSphere MQ démarré.

Activation de la trace de l'activité des applications MQI

Pourquoi et quand exécuter cette tâche

Pour pouvoir afficher les données de suivi des transactions dans les tableaux de bord de middleware et de topologie, la trace de l'activité des applications MQI doit être activée au niveau du gestionnaire de files d'attente.

Procédure

Pour activer la collecte des informations de trace de l'activité des applications MQI, exécutez la commande MQSC suivante :

```
ALTER QMGR ACTVTRC(ON)
```

Paramètres de sécurité de la surveillance éloignée

Pourquoi et quand exécuter cette tâche

Pour utiliser l'Agent WebSphere MQ pour surveiller un gestionnaire de files d'attente éloignées, vous devez vous assurer que les paramètres de sécurité d'IBM MQ (WebSphere MQ) n'empêchent pas l'agent de collecter les données de surveillance par l'intermédiaire d'un canal du système distant.

La procédure ci-après fournit un exemple de paramètre de sécurité simple pour la surveillance éloignée. Pour exercer un contrôle plus précis sur l'accès octroyé aux systèmes de connexion au niveau d'un canal, vous pouvez utiliser des enregistrements d'authentification de canal. Pour plus d'informations, voir la documentation sur les mécanismes de sécurité d'IBM MQ.

Procédure

1. Désactivez l'authentification de canal à l'aide de la commande MQSC suivante :
   ```
   ALTER QMGR CHLAUTH(DISABLED) CONNAUTH(' ')
   ```
2. Modifiez les paramètres de canal comme indiqué ci-après, *canal_moniteur_distant* représentant le nom du canal utilisé pour la surveillance éloignée.
   - Linux AIX
     ```
     ALTER CHANNEL(canal_moniteur_distant) CHLTYPE(SVRCONN) MCAUSER('mqm')
     ```
   - Windows
     ```
     ALTER CHANNEL(canal_moniteur_distant) CHLTYPE(SVRCONN) MCAUSER(MUSR_MQADMIN)
     ```
3. Actualisez les paramètres de sécurité.
   ```
   REFRESH SECURITY
   ```

Configuration de l'Agent WebSphere MQ

Vous devez attribuer un nom d'instance à l'Agent WebSphere MQ et configurer l'agent pour qu'il puisse commencer à surveiller votre environnement IBM MQ (WebSphere MQ).

Avant de commencer

- Assurez-vous que l'ID utilisateur de l'agent possède les droits appropriés lui permettant d'accéder aux objets IBM MQ (WebSphere MQ). Si ce n'est pas fait, suivez les instructions de la rubrique «ID utilisateur autorisés à exécuter l'agent», à la page 854.

- Configurez IBM MQ (WebSphere MQ) de sorte à activer la collecte de données requise. Si ce n'est pas fait, consultez «Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données», à la page 855.
- Vous devez fournir le nom du gestionnaire de files d'attente que l'Agent WebSphere MQ doit surveiller. Contactez l'administrateur IBM MQ (WebSphere MQ) si vous ne connaissez pas le nom du gestionnaire de files d'attente approprié. Sinon, exécutez la commande **dspmq** à partir du répertoire `bin` dans le répertoire d'installation d'IBM MQ (WebSphere MQ) pour obtenir la liste des gestionnaires de files d'attente. Vous devez fournir la valeur QMNAME renvoyée lorsque vous configurez l'Agent WebSphere MQ.

Pourquoi et quand exécuter cette tâche

L'Agent WebSphere MQ est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement.

Sur les systèmes UNIX ou Linux, vous pouvez choisir de configurer l'agent avec ou sans interactions. Sur les systèmes Windows, vous pouvez configurer l'agent sans interactions uniquement.

- Pour configurer l'agent avec interaction, exécutez le script de configuration et répondez aux invites. Voir «Configuration interactive».
- Pour configurer l'agent sans interaction, éditez le fichier de réponses silencieux, puis exécutez le script de configuration. Voir «Configuration en mode silencieux», à la page 859.

Important : Si vous avez également installé Monitoring Agent for WebSphere MQ, qui est fourni comme composant dans le produit ITCAM for Applications, sur le même système que l'Agent WebSphere MQ, fourni dans Cloud APM, ne les utilisez pas pour surveiller le même gestionnaire de files d'attente sur le système.

Configuration interactive

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Entrez la commande suivante pour créer une instance d'agent :

   rép_install`/bin/mq-agent.sh config` *nom_instance*

   où *nom_instance* est le nom à attribuer à l'instance.
2. A l'invite `Queue Manager Name`, indiquez le nom du gestionnaire de files d'attente à surveiller.
3. A l'invite `Nom de l'agent`, indiquez le nom d'agent à utiliser comme qualificatif intermédiaire du nom de système géré. N'appuyez pas sur la touche Entrée pour ignorer la spécification de ce paramètre.

   A faire : Ce nom d'agent est différent du nom d'instance d'agent. Le nom d'instance d'agent est utilisé dans le nom du fichier de configuration d'agent afin de distinguer les fichiers de configuration entre les agents, par exemple, *nom_hôte*`_mq_`*nom_instance*`.cfg`. Le nom d'agent est utilisé comme identificateur court pour créer des noms de système géré uniques. Pour savoir à quel moment un nom de système géré unique est requis, voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 860.
4. Si vous souhaitez surveiller un gestionnaire de files d'attente éloignées, spécifiez les paramètres de configuration ci-après. Si vous souhaitez surveiller un gestionnaire de files d'attente locales, appuyez sur la touche Entrée pour continuer.
   - `Connection Name` : nom de connexion de la surveillance éloignée. Le format est *adresse_IP*`(`*numéro_port*`)`. Par exemple, `127.0.0.1(1414)`. Si vous configurez l'instance d'agent pour la première fois, vous pouvez appuyer sur la touche Entrée pour accepter la valeur par défaut (null). Le nom de connexion approprié peut être détecté automatiquement.

- `Channel` : nom du canal utilisé pour la collecte de données à distance. Si vous configurez l'instance d'agent pour la première fois, vous pouvez appuyer sur la touche Entrée pour accepter la valeur par défaut (null). Le canal SYSTEM.DEF.SVRCONN est utilisé.

Limitation : Les journaux d'erreurs d'un gestionnaire de files d'attente éloignées ne peuvent pas être surveillés. Si l'agent surveille un gestionnaire de files d'attente éloignées, le tableau de bord MQ Errors Details ne contient pas de données.

5. Lorsque vous êtes invité à saisir le chemin d'accès à la bibliothèque WebSphere MQ, appuyez sur Entrée pour accepter la valeur par défaut, qui est le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) automatiquement découvert par l'Agent WebSphere MQ. Si aucune valeur par défaut n'est affichée, vous devez fournir le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour poursuivre. Par exemple, `/opt/mqm8/lib64` est le chemin d'accès à la bibliothèque 64 bits pour un système Linux.
6. Pour démarrer l'agent, entrez la commande suivante :
   rép_install`/bin/mq-agent.sh start` *nom_instance*

Configuration en mode silencieux

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

1. Ouvrez le fichier `mq_silent_config.txt` dans un éditeur de texte.
   - Linux AIX *rép_install*`/samples/mq_silent_config.txt`
   - Windows *rép_install*`\tmaitm6_x64\samples\mq_silent_config.txt`

   où *rép_install* correspond au répertoire d'installation de l'Agent WebSphere MQ.
2. Obligatoire : Pour **QMNAME**, indiquez le nom du gestionnaire de files d'attente à surveiller.
3. Obligatoire : Pour **AGTNAME**, indiquez le nom d'agent à utiliser comme qualificatif intermédiaire du nom de système géré.

   A faire : Ce nom d'agent est différent du nom d'instance d'agent. Le nom d'instance d'agent est utilisé dans le nom du fichier de configuration d'agent afin de distinguer les fichiers de configuration entre les agents, par exemple, *nom_hôte*`_mq_`*nom_instance*`.cfg`. Le nom d'agent est utilisé comme identificateur court pour créer des noms de système géré uniques. Pour savoir à quel moment un nom de système géré unique est requis, voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 860.
4. Si vous souhaitez surveiller un gestionnaire de files d'attente éloignées, spécifiez les paramètres de configuration suivants :
   - **CONNAME** : nom de connexion de la surveillance éloignée. Le format est *adresse_IP* (*numéro_port*). Par exemple, `127.0.0.1(1414)`.
   - **CHANNEL** : nom du canal utilisé pour la collecte de données à distance. S'il n'est pas spécifié, le canal SYSTEM.DEF.SVRCONN est utilisé.

   Limitation : Les journaux d'erreurs d'un gestionnaire de files d'attente éloignées ne peuvent pas être surveillés. Si l'agent surveille un gestionnaire de files d'attente éloignées, le tableau de bord MQ Errors Details ne contient pas de données.
5. Facultatif : Pour **WMQLIBPATH**, indiquez le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ). Par exemple, `/opt/mqm8/lib64`. Si aucune valeur n'est indiquée, le chemin d'accès peut être reconnu automatiquement au cours de la configuration de l'agent.
6. Sauvegardez et fermez le fichier `mq_silent_config.txt`, puis exécutez la commande suivante à partir de la ligne de commande :
   - Linux AIX *rép_install*`/bin/mq-agent.sh config` *nom_instance* *chemin_fichier_réponses*

- Windows *rép_install*\BIN\mq-agent.bat config *nom_instance* "*chemin_vers_fichier_réponses*"

où *nom_instance* est le nom de l'instance que vous configurez et *chemin_ fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

A faire : Sur les systèmes Windows, n'omettez pas les guillemets doubles ("") qui entourent le chemin d'accès du fichier de réponses silencieux, surtout lorsque le chemin d'accès contient des caractères spéciaux.
Par exemple, si le fichier de réponses se trouve dans le répertoire par défaut, lancez la commande suivante.

- Linux AIX

```
/opt/ibm/apm/agent/bin/mq-agent.sh config nom_instance
/opt/ibm/apm/agent/samples/mq_silent_config.txt
```

- Windows

```
C:\IBM\APM\BIN\mq-agent.bat config nom_instance
"C:\IBM\APM\tmaitm6_x64\samples\mq_silent_config.txt"
```

7. Pour démarrer l'agent, entrez la commande suivante :

- Linux AIX

```
rép_install/bin/mq-agent.sh start nom_instance
```

- Windows

```
rép_install\bin\mq-agent.bat start nom_instance
```

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent WebSphere MQ au Tableau de bord d'Application Performance. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 989. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1145.

Que faire ensuite

- Si vous avez activé la collecte des informations de trace de l'activité des applications MQI au niveau du gestionnaire de files d'attente, utilisez la page Configuration d'agent pour configurer l'Agent WebSphere MQ de sorte à collecter les données de suivi des transactions du gestionnaire de files d'attente surveillé. Voir «Configuration du suivi des transactions pour l'Agent WebSphere MQ», à la page 862. Si l'agent ne figure pas sur la page Configuration d'agent, redémarrez le serveur Cloud APM.
- En fonction de vos exigences en termes de surveillance, vous pourriez avoir besoin d'un nom de système géré unique pour distinguer les agents de surveillance. Utilisez l'option `Agent Name` dans la commande `mq-agent.sh config` pour spécifier le qualificatif intermédiaire du nom de système géré. Voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente».
- Pour configurer l'Agent WebSphere MQ pour la surveillance éloignée, vous devez effectuer certaines tâches de configuration manuelle après avoir créé une instance d'agent. Pour connaître les instructions, consultez les rubriques suivantes :
  - «Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance», à la page 864
  - «Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance», à la page 866

Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente

Parfois, il est nécessaire d'utiliser des noms de système géré uniques afin de différencier des agents de surveillance qui se connectent au même serveur Cloud APM. Utilisez le paramètre **AGTNAME** dans le fichier

de réponses silencieux ou l'option `Nom de l'agent` dans la commande **mq-agent.sh config** pour indiquer le qualificatif intermédiaire utilisé dans le nom de système géré.

Pourquoi et quand exécuter cette tâche

Au démarrage de l'Agent WebSphere MQ, ce dernier enregistre le système géré suivant :
nomgestionnairefilesd'attentesurveillé:*nomagent*:MQ

où

- *nomgestionnairefilesd'attentesurveillé* correspond au nom du gestionnaire de files d'attente surveillé par l'agent.
- *nomagent* correspond au qualificatif intermédiaire du nom de système géré. Si la valeur *nomagent* n'est pas spécifiée, aucune valeur n'est utilisée.

La spécification de la valeur du nom de l'agent s'avère utile dans les cas suivants :

- Si votre site comporte plusieurs gestionnaires de files d'attente ayant le même nom et s'exécutant sur des noeuds différents, spécifiez le nom de l'agent pour chaque gestionnaire de files d'attente afin que l'Agent WebSphere MQ puisse créer des noms de système géré uniques.
- Si le nom du système géré comporte plus de 32 caractères, 2 noms de gestionnaires de files d'attente différents peuvent être résolus sur le même nom en raison de sa troncature. Pour distinguer les noms de système géré des gestionnaires de files d'attente, indiquez un nom d'agent pour chaque gestionnaire de files d'attente.
- Si vous voulez grouper et identifier les noms de gestionnaire de files d'attente par autre chose que le nom d'hôte et le nom de gestionnaire de files d'attente, comme le nom de cluster haute disponibilité.
- Si vous voulez configurer plusieurs agents connectés au même serveur Cloud APM de sorte qu'ils surveillent les gestionnaires de files d'attente avec le même nom sur des hôtes différents.

Configuration interactive

Procédure

Pour utiliser l'option `Nom de l'agent` dans la commande **mq-agent.sh config**, procédez comme suit :

1. Sur la ligne de commande, exécutez la commande suivante pour lancer la configuration de l'Agent WebSphere MQ.

   ```
   ./mq-agent.sh config nom_instance
   ```

   où *nom_instance* est le nom de l'instance que vous avez démarrée.
2. Suivez les options pour configurer l'instance d'agent. Le nom du gestionnaire de files d'attente est obligatoire. Pour les autres options, si aucune modification n'est nécessaire, utilisez la valeur par défaut.
3. Lorsque l'option `Nom de l'agent` apparaît, indiquez le qualificateur intermédiaire du nom du système géré.

   A faire : Le nom de système géré complet est *nomgestionnairefilesd'attentesurveillé*:*nomagent*:MQ. La longueur maximale pour le nom de système géré complet est de 32 caractères, ce qui signifie que la longueur maximale du qualificateur intermédiaire *nomagent* dépend de la longueur du nom du gestionnaire de files d'attente. Si la valeur spécifiée pour l'option `Nom de l'agent` dépasse la longueur maximale, la valeur de *nomagent* est tronquée à 8 caractères.
   Par exemple, pour surveiller un gestionnaire de files d'attente nommé PERSONNEL sur le noeud AIX1 et qu'un autre gestionnaire nommé PERSONNEL se trouve sur un noeud nommé LINUX2, exécutez la commande suivante pour le noeud AIX1 en premier :

   ```
   ./mq-agent.sh config PERSONNEL
   ```

   Indiquez ensuite le nom de l'agent lorsque l'option *Nom de l'agent* apparaît :

```
Nom de l'agent (par défaut : ) : AIX1
```

Pour surveiller simultanément le gestionnaire de files d'attente PERSONNEL sur le noeud LINUX2, exécutez la commande suivante en premier :

```
./mq-agent.sh config PERSONNEL
```

Indiquez ensuite le nom de l'agent :

```
Nom de l'agent (par défaut : ) : LINUX2
```

A faire : Les noms des noeuds d'agent sont utilisés pour l'option `Nom de l'agent` dans les exemples de code à des fins explicatives uniquement. Vous pouvez spécifier d'autres chaînes pour l'option `Nom de l'agent`.

Configuration en mode silencieux

Procédure

Pour utiliser le paramètre **AGTNAME** dans le fichier de réponses silencieux, procédez comme suit :

1. Ouvrez le fichier de réponses silencieux `mq_silent_config.txt` dans un éditeur de texte.
2. Indiquez un nom d'agent pour le paramètre **AGTNAME**.

   A faire : Le nom de système géré complet est *nomgestionnairefilesd'attentesurveillé*:*nomagent*:MQ. La longueur maximale pour le nom de système géré complet est de 32 caractères, ce qui signifie que la longueur maximale du qualificateur intermédiaire *nomagent* dépend de la longueur du nom du gestionnaire de files d'attente. Si la valeur indiquée pour le paramètre **AGTNAME** dépasse la longueur maximale autorisée, la valeur de *nomagent* est tronquée à 8 caractères.
3. Sauvegardez et fermez le fichier `mq_silent_config.txt`, puis exécutez la commande suivante à partir de la ligne de commande :

   ```
   rép_install/BIN/mq-agent.sh config nom_instance chemin_fichier_réponses
   ```

   où *nom_instance* est le nom de l'instance que vous configurez et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

Que faire ensuite

Connectez vous à console Cloud APM. Si l'instance d'agent portant l'ancien nom de système géré apparaît toujours comme déconnectée, éditez votre application pour la supprimer, puis ajoutez la nouvelle instance d'agent portant le nom d'agent attribué.

Configuration du suivi des transactions pour l'Agent WebSphere MQ

Vous pouvez afficher les données de suivi des transactions d'IBM MQ (WebSphere MQ) dans les tableaux de bord de topologie et du middleware après avoir activé la collecte de données sur la page Configuration d'agent pour l'Agent WebSphere MQ.

Avant de commencer

- Assurez-vous que la collecte des informations de trace de l'activité des applications MQI est activée au niveau du gestionnaire de files d'attente. Si ce n'est pas fait avant d'avoir configuré et démarré l'Agent WebSphere MQ, suivez les instructions de la rubrique «Activation de la trace de l'activité des applications MQI», à la page 857, puis redémarrez l'agent.
- Assurez-vous que la version d'IBM MQ (WebSphere MQ) que vous utilisez est prise en charge par la fonction de suivi des transactions. Pour les informations les plus récentes sur les versions d'IBM MQ (WebSphere MQ) prises en charge, voir la déclaration des prérequis dans le rapport détaillé sur la configuration système requise pour l'Agent WebSphere MQ.
- Assurez-vous que l'Agent WebSphere MQ est configuré pour surveiller le gestionnaire de files d'attente. Pour plus d'informations, voir «Configuration de l'Agent WebSphere MQ», à la page 857.

A faire : Vérifiez que vous avez mis à niveau l'Agent WebSphere MQ dans sa version la plus récente. Pour Cloud APM, Private, la version 8.1.2 ou ultérieure est requise. Vous devez mettre à niveau l'agent, de même que configurer et activer le suivi des transactions afin de visualiser les données dans certains des widgets, tels le widget Volume des messages.

Procédure

Pour configurer le suivi des transactions pour l'Agent WebSphere MQ, procédez comme suit :

1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Configuration d'agent**. La page Configuration d'agent s'affiche.
2. Cliquez sur l'onglet **WebSphere MQ**.
3. Cochez les cases des gestionnaires de files d'attente que vous voulez surveiller et effectuez l'une des actions suivantes de la liste **Actions** :
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled.

     Conseil : Le suivi des files d'attente alias et des files d'attente éloignées est activé par défaut. Pour réduire le volume de données faisant l'objet du suivi, vous pouvez désactiver le suivi des files d'attente alias et éloignées en cliquant sur **Set Alias Queue Tracking** > **Disabled** dans la liste **Actions**. Une fois le suivi des files d'attente alias et éloignées désactivé, ces files d'attente sont supprimées de la vue de topologie des transactions.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour et défini sur Disabled.

Résultats

Vous avez configuré l'Agent WebSphere MQ pour le suivi des gestionnaires de files d'attente sélectionnés. Les données de suivi des transactions peuvent être affichées dans les tableaux de bord de topologie et de middleware. Pour plus d'informations, voir «Ajout d'applications middleware au Tableau de bord d'Application Performance», à la page 107.

Activation de la collecte de données pour l'historique à long terme de files d'attente et de canal

Par défaut, l'historique à long terme de file d'attente et de canal n'est pas collecté et n'est pas affiché dans les tableaux de bord ou widgets de groupe prédéfinis. Toutefois, vous pouvez activer l'agent pour la collecte des données d'historique à long terme, et utiliser ensuite l'onglet **Détails d'attribut** pour interroger les données collectées.

Avant de commencer

Vérifiez que l'Agent WebSphere MQ est installé et configuré. Pour plus d'informations, voir «Configuration de l'Agent WebSphere MQ», à la page 857.

Pourquoi et quand exécuter cette tâche

Les données d'historique à long terme de canal ou de file d'attente peuvent être utiles pour détecter les problèmes liés à des canaux ou files d'attente individuels.

Si vous êtes un utilisateur de Tivoli Data Warehouse, l'agent peut également envoyer les données d'historique à long terme à Tivoli Data Warehouse pour un traitement supplémentaire.

Procédure

Exécutez les étapes suivantes pour permettre à l'Agent WebSphere MQ de collecter les données d'historique à long terme de file d'attente ou de canal :

1. Ouvrez le ficher d'environnement suivant avec un éditeur de texte. Si le fichier `mq.environment` n'existe pas, créez-le vous-même.
   - Linux AIX *rép_install*`/config/mq.environment`
   - Windows *rép_install*`\Config\KMQENV_`*instance*

   où :
   - *rép_install* est le répertoire d'installation de l'agent. Par défaut, il s'agit de `/opt/ibm/apm` sur les systèmes Linux et AIX, et de `C:\IBM\APM` sur les systèmes Windows.
   - *instance* est le nom de l'instance d'agent.
2. Activez la collecte de données en définissant **LH_COLLECTION** à la valeur `ENABLED`.
   ```
   LH_COLLECTION=ENABLED
   ```
3. Facultatif : Si vous êtes un utilisateur de Tivoli Data Warehouse et souhaitez que l'agent envoie les données collectées à Tivoli Data Warehouse, définissez **LH_PVTHISTORY** à la valeur `ENABLED`.
   ```
   LH_PVTHISTORY=ENABLED
   ```

   A faire : Activez cette option uniquement si les données collectées doivent être envoyées à Tivoli Data Warehouse.
4. Sauvegardez votre modification et redémarrez l'agent.

Résultats

L'Agent WebSphere MQ commence à collecter les données d'historique à long terme de file d'attente et de canal. Si vous avez spécifié `LH_PVTHISTORY=ENABLED`, les données d'historique à long terme collectées peuvent également être envoyées à Tivoli Data Warehouse.

Que faire ensuite

Utilisez l'onglet **Détails d'attribut** pour afficher les données collectées dans le tableau de bord de l'instance d'agent configurée. Sélectionnez **Channel_Long-Term_History** ou **Queue_Long-Term_History** dans la liste **Jeu de données**. Pour plus d'informations sur l'onglet **Détails d'attribut**, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1140.

Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance

Vous pouvez utiliser l'Agent WebSphere MQ pour surveiller le gestionnaire de files d'attente éloignées dans l'environnement MQ Appliance. Pour ce faire, vous devez configurer une instance d'agent et configurer les connexions entre l'agent et le gestionnaire de file d'attente.

Avant de commencer

Vous devez créer une instance de l'Agent WebSphere MQ pour la surveillance à distance. Pour obtenir des instructions, voir «Configuration de l'Agent WebSphere MQ», à la page 857.

Procédure

1. Ouvrez l'un des fichiers de configuration d'agent suivants en fonction de votre système d'exploitation :
   - Windows *rép_install*`\TMAITM6_x64\mq_<`*nom_instance*`>.cfg`
   - Linux AIX *rép_install*`/config/`*nom_hôte*`_mq_`*gest_file_att_éloign*`.cfg`

2. Modifiez le fichier de configuration de l'instance d'agent de sorte à activer la surveillance éloignée en remplaçant son contenu par les lignes suivantes :

```
SET   GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(gest_file_att_éloign) REMOTE(YES)
SET AGENT NAME(IDagent)
SET QUEUE NAME(*) MGRNAME(gest_file_att_éloign) QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(gest_file_att_éloign)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

où :

- *gest_file_att_éloign* est le nom du gestionnaire de files d'attente éloignées.
- *IDagent* est l'ID qui identifie le système du gestionnaire de file d'attente. Il s'agit généralement du nom d'hôte ou de l'adresse IP du système distant sur lequel le gestionnaire de file d'attente s'exécute.

3. Exécutez les commandes suivantes sur le système distant où le gestionnaire de file d'attente est installé afin de définir un canal client, un canal de connexion serveur et un programme d'écoute sur le gestionnaire de files d'attente éloignées pour établir une communication avec l'agent de surveillance :

```
M2000# mqcli
M2000(mqcli)#runmqsc gest_file_att_éloign
> DEFINE LISTENER(prog_écoute) TRPTYPE(TCP) PORT(num_port)
> DEFINE CHANNEL(nom_canal)CHLTYPE(SVRCONN) TRPTYPE(TCP)
> DEFINE CHANNEL(nom_canal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port)') QMNAME(gest_file_att_éloign)
> END
```

où :

- *gest_file_att_éloign* est le nom du gestionnaire de files d'attente éloignées.
- *prog_écoute* est le nom du programme d'écoute sur le gestionnaire de files d'attente éloignées.
- *num_port* est le numéro de port à utiliser pour le programme d'écoute.
- *nom_canal* est le nom que vous attribuez au canal serveur et au canal client.
- *IP_hôte* est l'adresse IP du système distant.

4. Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour le gestionnaire de file d'attente à l'aide de la commande **runmqsc** ou **runmqsc -n**.

Conseil :

- Si IBM MQ (WebSphere MQ) version 8.0 ou ultérieure est installé sur le système où l'Agent WebSphere MQ est en cours d'exécution, vous pouvez utiliser la commande suivante pour créer le fichier AMQCLCHL.TAB pour la surveillance éloignée :

```
runmqsc -n
> DEFINE CHANNEL(nom_canal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
> CONNAME('IP_hôte(num_port)') QMNAME(gest_file_att_éloign)
> END
```

- Pour surveiller les gestionnaires de file d'attente haute disponibilité sur MQ Appliance, vous pouvez utiliser une instance d'agent pour vous connecter à un système doté du gestionnaire de file d'attente actif. Pour ce faire, créez deux fichiers de table de définition de canal du client pour les gestionnaires de file d'attente haute disponibilité (un fichier pour chaque adresse IP).

```
runmqsc -n
> DEFINE CHANNEL(nom_canal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP1_hôte(num_port)') QMNAME(gest_file_att_hd)
> DEFINE CHANNEL(nom_canal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP2_hôte(num_port)') QMNAME(gest_file_att_hd)
> END
```

5. Transférez le fichier AMQCLCHL.TAB en mode binaire vers le système où l'Agent WebSphere MQ est installé. Pour ce faire, vous pouvez utiliser la fonction File Management de l'interface utilisateur d'IBM MQ Console. Sur les systèmes Linux ou UNIX, vous pouvez également utiliser la commande suivante :

   ```
   M2000#config
   M2000(config)#copy mqbackup:///qmgr_AMQCLCHL.TAB scp://nom_utilisateur@adresse_IP/
   [/]répertoire_dest
   ```

   Conseil : Le répertoire de destination varie en fonction du système d'exploitation sur lequel l'Agent WebSphere MQ est installé.

   - Windows *rép_install*\TMAITM6_x64
   - Linux AIX *rép_install/arch*/mq/bin

6. Renommez qmgr_AMQCLCHL.TAB en AMQCLCHL.TAB.
7. Configurez le programme d'écoute de sorte qu'il démarre automatiquement, puis démarrez le programme d'écoute sur le gestionnaire de files d'attente éloignées en exécutant les commandes suivantes sur le système distant :

   ```
   M2000# mqcli
   M2000(mqcli)#runmqsc gest_file_att_éloign
   > ALTER LISTENER(prog_écoute) TRPTYPE(tcp) CONTROL(gest_file_att_éloign)
   > START LISTENER(prog_écoute)
   > END
   ```

8. Vérifiez que les paramètres d'authentification de canal sont correctement configurés pour l'ID utilisateur utilisé pour configurer la connexion entre l'instance d'agent et le gestionnaire de file d'attente.
9. Démarrez tous les programmes d'écoute pour le gestionnaire de file d'attente surveillé à distance et démarrez l'Agent WebSphere MQ.

Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance

Pour surveiller le gestionnaire de file d'attente haute disponibilité à distance sur MQ Appliance, vous avez deux options. La première option consiste à utiliser une instance d'agent unique pour vous connecter à un système doté du gestionnaire de file d'attente actif. La seconde option consiste à utiliser une instance d'agent distincte pour chaque dispositif sur lequel le gestionnaire de file d'attente pourrait s'exécuter.

Pourquoi et quand exécuter cette tâche

Seule la seconde option est décrite ici. Pour utiliser les différentes instances d'agent, vous avez besoin de deux installations de l'Agent WebSphere MQ sur les systèmes Linux ou UNIX. Sur les systèmes Windows, vous n'avez besoin que d'une installation de l'agent et vous devez créer des instances d'agent distinctes.

Procédure

- Linux AIX Procédez comme suit pour utiliser l'Agent WebSphere MQ installé sur les systèmes Linux ou UNIX pour la surveillance éloignée :
  1. Installez l'Agent WebSphere MQ dans différents répertoires sur le système.
  2. Créez une instance de chaque Agent WebSphere MQ installé. Pour obtenir des instructions, voir «Configuration de l'Agent WebSphere MQ», à la page 857.

3. Modifiez le fichier de configuration de chaque instance d'agent de sorte à activer la surveillance éloignée en remplaçant son contenu par les lignes suivantes :

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(nom_gest_file_att) REMOTE(YES)
SET AGENT NAME(IDagent)
SET QUEUE NAME(*) MGRNAME(nom_gest_file_att) QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(nom_gest_file_att)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

   Où :

   – *nom_gest_file_att* est le nom du gestionnaire de files d'attente haute disponibilité.
   – *IDagent* est l'ID qui identifie le système du gestionnaire de file d'attente. Il s'agit généralement du nom d'hôte ou de l'adresse IP du système distant sur lequel le gestionnaire de file d'attente haute disponibilité s'exécute.

   Le nom et le chemin d'accès du fichier de configuration sont les suivants : *rép_install*/config/*nom_hôte*_mq_*nom_gest_file_att*.cfg.

4. Créez une paire de canaux client et serveur entre le gestionnaire de file d'attente principal et l'Agent WebSphere MQ et entre le gestionnaire de file d'attente secondaire et l'Agent WebSphere MQ sur le système distant où le gestionnaire de file d'attente principal est installé.

   A faire : Vous devez exécuter toutes les commandes suivantes avant de passer à l'étape suivante.

   a. Exécutez les commandes suivantes pour le gestionnaire de file d'attente principal :

```
M2000# mqcli
M2000(mqcli)#runmqsc gest_file_att_principal
>DEFINE LISTENER(prog_écoute_principal) TRPTYPE(TCP) PORT(num_port_principal)
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port_principal)') QMNAME(gest_file_att_principal)
```

      où :

      – *gest_file_att_principal* est le nom du gestionnaire de files d'attente principal.
      – *prog_écoute_principal* est le nom du programme d'écoute pour le gestionnaire de files d'attente principal.
      – *num_port_principal* est le numéro du port utilisé par le programme d'écoute.
      – *nom_canal_principal* est le nom que vous attribuez au canal serveur et au canal client.
      – *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente principal est installé.

   b. Exécutez les commandes suivantes pour le gestionnaire de file d'attente secondaire sur le gestionnaire de file d'attente principal. Cette opération permet d'ajouter les informations de connexion pour le gestionnaire de file d'attente secondaire au fichier de table de définition de canal du client du gestionnaire de file d'attente principal. Le même agent peut ensuite se connecter au gestionnaire de file d'attente secondaire automatiquement lorsque le gestionnaire de file d'attente principal procède à une reprise en ligne.

```
>DEFINE LISTENER(prog_écoute_secondaire) TRPTYPE(TCP) PORT(num_port_secondaire)
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port_secondaire)') QMNAME(gest_file_att_secondaire)
```

      où :

– *gest_file_att_secondaire* est le nom du gestionnaire de file d'attente secondaire sur le système distant. Il est identique au nom du gestionnaire de files d'attente principal.
– *prog_écoute_secondaire* est le nom du programme d'écoute pour le gestionnaire de files d'attente secondaire.
– *num_port_secondaire* est le numéro du port utilisé par le programme d'écoute.
– *nom_canal_secondaire* est le nom que vous attribuez au canal serveur et au canal client.
– *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente secondaire est installé.

c. Enfin, exécutez la commande suivante :

```
>END
>EXIT
```

5. Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour l'instance de l'Agent WebSphere MQ sur le premier dispositif MQ.
   a. Utilisez la commande **runmqsc** ou **runmqsc -n** pour créer le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le premier dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif1(num_port_principal)') QMNAME(nom_gest_file_att)
```

   où *IP_hôte_dispositif1* est l'adresse IP du premier dispositif MQ ; les valeurs de *nom_canal_principal* et *num_port_principal* sont identiques à celles que vous avez définies à l'étape 4.

   Conseil : Par défaut, le fichier AMQCLCHL.TAB est créé dans le répertoire var/mqm/qmgrs/*nom_gest_file_att*/@ipcc.

   b. Déplacez le fichier AMQCLCHL.TAB principal dans le répertoire *rép_install_agent*/*arch*/mq/bin sur le système où l'Agent WebSphere MQ est installé pour le gestionnaire de files d'attente principal.
6. Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour l'instance de l'Agent WebSphere MQ sur le deuxième dispositif MQ.
   a. Utilisez la commande **runmqsc** ou **runmqsc -n** pour créer le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le deuxième dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif2(num_port_secondaire)') QMNAME(nom_gest_file_att)
```

   où *IP_hôte_dispositif2* est l'adresse IP du deuxième dispositif MQ ; les valeurs de *nom_canal_secondaire* et *num_port_secondaire* sont identiques à celles que vous avez définies à l'étape 4.

   b. Déplacez le fichier AMQCLCHL.TAB secondaire dans le répertoire *rép_install_agent*/*arch*/mq/bin sur le système où l'Agent WebSphere MQ est installé pour le gestionnaire de files d'attente secondaire.
7. Vérifiez que les paramètres d'authentification de canal sont correctement configurés pour l'ID utilisateur utilisé pour configurer la connexion entre l'instance d'agent et le gestionnaire de file d'attente.
8. Démarrez tous les programmes d'écoute pour le gestionnaire de file d'attente surveillé à distance et démarrez toutes les instances de l'Agent WebSphere MQ.

- Windows Procédez comme suit pour utiliser l'Agent WebSphere MQ installé sur les systèmes Windows pour la surveillance éloignée :
  1. Installez l'Agent WebSphere MQ sur le système Windows.
  2. Créez deux instances de l'Agent WebSphere MQ pour chaque gestionnaire de file d'attente haute disponibilité.
  3. Modifiez le fichier de configuration de chaque instance d'agent de sorte à activer la surveillance éloignée en remplaçant son contenu par les lignes suivantes :

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(nom_gest_file_att) REMOTE(YES)
SET AGENT NAME(IDagent)
SET QUEUE NAME(*) MGRNAME(nom_gest_file_att) QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(nom_gest_file_att)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

Où :

- *nom_gest_file_att* est le nom du gestionnaire de files d'attente haute disponibilité.
- *IDagent* est l'ID qui identifie le système du gestionnaire de file d'attente. Il s'agit généralement du nom d'hôte ou de l'adresse IP du système distant sur lequel le gestionnaire de file d'attente haute disponibilité s'exécute.

Conseil : Le nom et le chemin d'accès du fichier de configuration sont les suivants : *rép_install*\TMAITM6_x64\mq_<*nom_instance*>.cfg.

4. Créez une paire de canaux client et serveur entre le gestionnaire de file d'attente principal et l'Agent WebSphere MQ et entre le gestionnaire de file d'attente secondaire et l'Agent WebSphere MQ sur le système distant où le gestionnaire de file d'attente principal est installé.

   A faire : Vous devez exécuter toutes les commandes suivantes avant de passer à l'étape suivante.

   a. Exécutez les commandes suivantes pour le gestionnaire de file d'attente principal :

      ```
      M2000# mqcli
      M2000(mqcli)#runmqsc gest_file_att_principal
      >DEFINE LISTENER(prog_écoute_principal) TRPTYPE(TCP) PORT(num_port_principal)
      >DEFINE CHANNEL(nom_canal_principal) CHLTYPE(SVRCONN) TRPTYPE(TCP)
      >DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
      CONNAME('IP_hôte(num_port_principal)') QMNAME(gest_file_att_principal)
      ```

      où :

      - *gest_file_att_principal* est le nom du gestionnaire de files d'attente principal.
      - *prog_écoute_principal* est le nom du programme d'écoute pour le gestionnaire de files d'attente principal.
      - *num_port_principal* est le numéro du port utilisé par le programme d'écoute.
      - *nom_canal_principal* est le nom que vous attribuez au canal serveur et au canal client.
      - *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente principal est installé.

   b. Exécutez les commandes suivantes pour le gestionnaire de file d'attente secondaire sur le gestionnaire de file d'attente principal. Cette opération permet d'ajouter les informations de connexion pour le gestionnaire de file d'attente secondaire au fichier de table de définition de canal du client du gestionnaire de file d'attente principal. Le même agent peut ensuite se connecter au gestionnaire de file d'attente secondaire automatiquement lorsque le gestionnaire de file d'attente principal procède à une reprise en ligne.

      ```
      >DEFINE LISTENER(prog_écoute_secondaire) TRPTYPE(TCP) PORT(num_port_secondaire)
      >DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(SVRCONN) TRPTYPE(TCP)
      >DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
      CONNAME('IP_hôte(num_port_secondaire)') QMNAME(gest_file_att_secondaire)
      ```

      où :

      - *gest_file_att_secondaire* est le nom du gestionnaire de file d'attente secondaire sur le système distant. Il est identique au nom du gestionnaire de files d'attente principal.

- *prog_écoute_secondaire* est le nom du programme d'écoute pour le gestionnaire de files d'attente secondaire.
- *num_port_secondaire* est le numéro du port utilisé par le programme d'écoute.
- *nom_canal_secondaire* est le nom que vous attribuez au canal serveur et au canal client.
- *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente secondaire est installé.

c. Enfin, exécutez la commande suivante :

```
>END
>EXIT
```

5. Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour chaque instance de l'Agent WebSphere MQ.
   a. Utilisez la commande **runmqsc** ou **runmqsc -n** pour créer le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le premier dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif1(num_port_principal)') QMNAME(nom_gest_file_att)
```

   où *IP_hôte_dispositif1* est l'adresse IP du premier dispositif MQ ; les valeurs de *nom_canal_principal* et *num_port_principal* sont identiques à celles que vous avez définies à l'étape 4.

   b. Créez le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le deuxième dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif2(num_port_secondaire)') QMNAME(nom_gest_file_att)
```

   où *IP_hôte_dispositif2* est l'adresse IP du deuxième dispositif MQ ; les valeurs de *nom_canal_secondaire* et *num_port_secondaire* sont identiques à celles que vous avez définies à l'étape 4.

6. Attribuez aux deux fichiers AMQCLCHL.TAB des noms différents, par exemple, NODE1.TAB et NODE2.TAB. Transférez-les vers le répertoire *rép_install*\TMAITM6_x64, où *rép_install* est le répertoire d'installation de l'Agent WebSphere MQ.
7. Modifiez le fichier kmqcma_*nom_instance*.ini de sorte à définir la valeur de **MQCHLTAB** sur le fichier de table de définition de canal du client pour chaque instance d'agent. Par exemple, définissez MQCHLTAB=NODE1.TAB dans le fichier kmqcma_instance1.ini et MQCHLTAB=NODE2.TAB dans le fichier kmqcma_instance2.ini.
8. Ouvrez Windows Register Editor, localisez la clé **MQCHLTAB** et redéfinissez sa valeur AMQCLCHL.TAB sur le nom du fichier de table de définition de canal du client approprié pour chaque instance d'agent.
   - **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instance1*\Environment**
     MQCHLTAB=*NODE1.TAB*
   - **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instance2*\Environment**
     MQCHLTAB=*NODE2.TAB*
9. Vérifiez que les paramètres d'authentification de canal sont correctement configurés pour l'ID utilisateur utilisé pour configurer la connexion entre l'instance d'agent et le gestionnaire de file d'attente.
10. Démarrez tous les programmes d'écoute pour le gestionnaire de file d'attente surveillé à distance et démarrez toutes les instances de l'Agent WebSphere MQ.

Chapitre 11. Intégration à d'autres produits et composants

Vous pouvez intégrer d'autres produits et composants à IBM Cloud Application Performance Management afin d'obtenir une solution robuste.

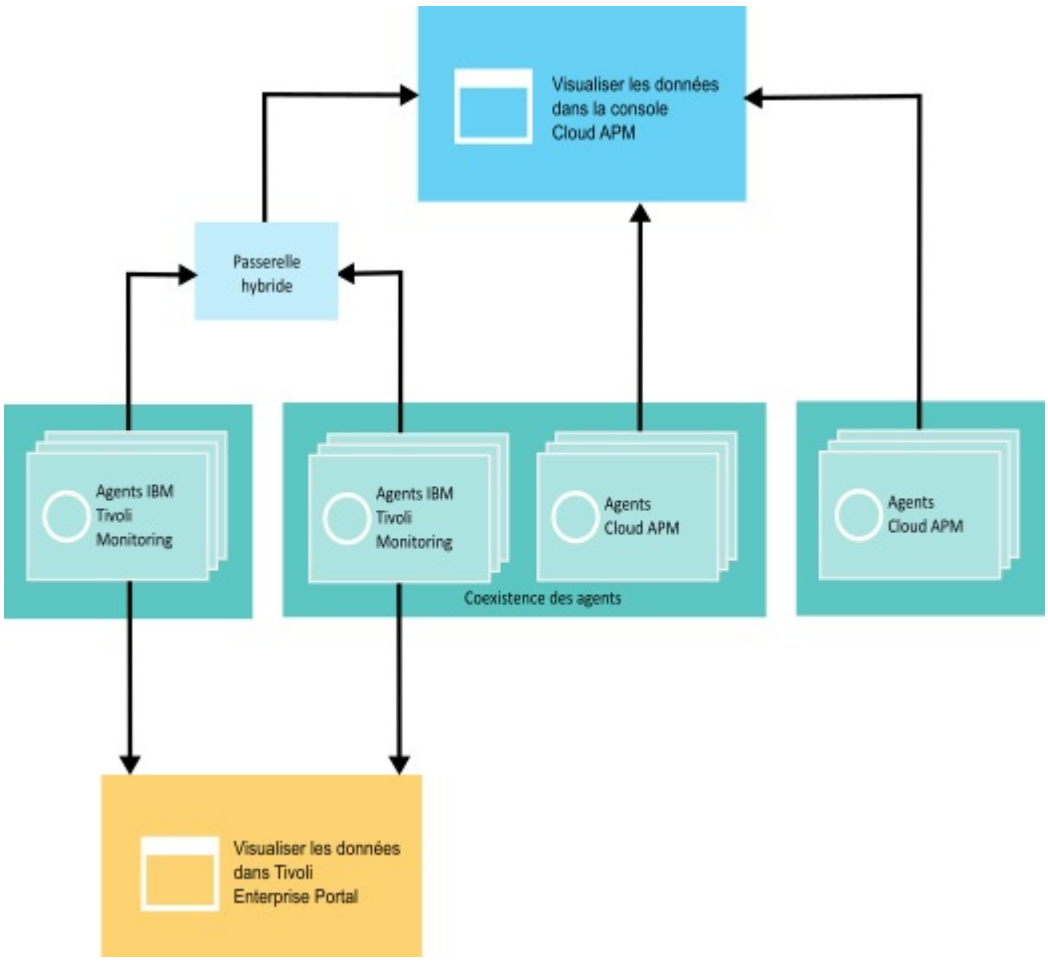
Intégration à IBM Tivoli Monitoring V6.3

Dans un environnement qui inclut les produits IBM Tivoli Monitoring et IBM Cloud Application Performance Management, vous pouvez utiliser ces produits ensemble de plusieurs façons.

Les options suivantes sont disponibles pour l'intégration à IBM Tivoli Monitoring :

- Vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management pour offrir une vue consolidée des systèmes gérés à partir d'un ou plusieurs domainesTivoli Monitoring et de votre domaine Cloud APM dans les pages du Tableau de bord d'Application Performance. Pour plus d'informations sur l'intégration des agents, voir «Passerelle hybride», à la page 875.
- Vous pouvez configurer les agents Cloud APM de sorte à envoyer les données d'historique à Tivoli Data Warehouse afin d'utiliser les outils de génération de rapports d'historique Tivoli Monitoring. Pour plus d'informations sur Tivoli Data Warehouse, voir «Tivoli Data Warehouse pour le rapport de l'historique», à la page 888.
- Vous pouvez installer des agents Tivoli Monitoring et Cloud APM sur le même système. Lorsque des agents coexistent sur le même ordinateur, mais ne sont pas dans le même répertoire, les données des agents Cloud APM sont disponibles dans la console Cloud APM et les données des agents Tivoli Monitoring sont disponibles dans Tivoli Enterprise Portal. Si des agents coexistants surveillent les mêmes ressources, certaines limitations s'appliquent. Pour plus d'informations sur la coexistence d'agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 872.

© Copyright IBM Corp. 2015, 2018



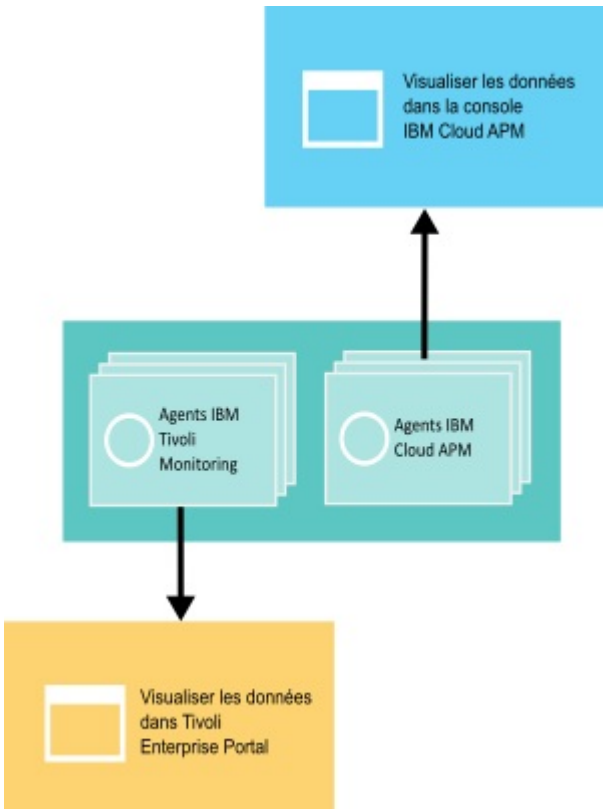
Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire.

Les agents Cloud APM sont mentionnés sous le nom d'agents de la version 8. Les agents Tivoli Monitoring sont mentionnés sous le nom d'agents de la version 6 ou 7.

Lorsque des agents coexistent sur le même ordinateur, les données issues des agents version 8 sont disponibles dans la console Cloud APM et les données issues des agents version 6 ou 7 sont disponibles dans Tivoli Enterprise Portal.

Lorsque des agents version 6 ou 7 qui coexistent sur le même ordinateur que des agents version 8 et qui surveillent différentes ressources, sont intégrés à la Passerelle hybride d'IBM Cloud Application Performance Management, les données issues des deux versions d'agents sont disponibles dans la console Cloud APM. Pour plus d'informations, voir «Passerelle hybride», à la page 875.



Le tableau suivant dresse la liste des agents Tivoli Monitoring avec des liens de documentation :

Tableau 200. Liens de documentation pour les agents Tivoli Monitoring

Agents Tivoli Monitoring	**Liens de documentation**
IBM Monitoring Agent for Citrix Virtual Desktop Infrastructure	Knowledge Center d'IBM Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring for Virtual Environments Agent for Cisco UCS	Knowledge Center de Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines	Knowledge Center de Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring for Virtual Environments Agent for VMware VI	Knowledge Center de Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring: HMC Base Agent	Knowledge Center d'IBM Tivoli Monitoring
IBM Tivoli Monitoring: Linux OS Agent	Knowledge Center de Tivoli Monitoring
IBM Tivoli Monitoring: UNIX OS Agent	Knowledge Center de Tivoli Monitoring
IBM Tivoli Monitoring : Agent Windows OS	Knowledge Center de Tivoli Monitoring
ITCAM Agent for DB2	Knowledge Center d'ITCAM for Applications
Agent ITCAM pour les serveurs HTTP	Knowledge Center d'ITCAM for Applications
ITCAM Agent for J2EE	Knowledge Center d'ITCAM for Applications
ITCAM for Microsoft Applications : agent Microsoft Active Directory	Knowledge Center d'IBM Tivoli Composite Application Manager for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft Cluster Server Agent	Knowledge Center d'ITCAM for Microsoft Applications

Tableau 200. Liens de documentation pour les agents Tivoli Monitoring (suite)

Agents Tivoli Monitoring	Liens de documentation
ITCAM for Microsoft Applications: Microsoft Exchange Server Agent	Knowledge Center d'ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft Hyper-V Server Agent	Knowledge Center d'ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft Internet Information Services Agent	Knowledge Center d'ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Skype for Business Server Agent	Knowledge Center d'ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft .NET Framework Agent	Knowledge Center d'ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft SharePoint Server Agent	Knowledge Center d'ITCAM for Microsoft Applications
Monitoring Agent for Microsoft SQL Server	Knowledge Center d'ITCAM for Microsoft Applications
ITCAM Agent for SAP Applications	Knowledge Center d'ITCAM for Applications
ITCAM Agent for WebSphere Applications	Knowledge Center d'IBM Tivoli Composite Application Manager for Application Diagnostics pour les versions 7.1 et précédentes et dans le Knowledge Center d'ITCAM for Applications pour les versions 7.2 et suivantes.
ITCAM Agent for WebSphere DataPower Appliance	Knowledge Center d'IBM Tivoli Composite Application Manager for Applications
Monitoring Agent for WebSphere Message Broker	Knowledge Center d'ITCAM for Applications
Monitoring Agent for WebSphere MQ	Knowledge Center d'ITCAM for Applications
ITCAM Extended Agent for Oracle Database	Knowledge Center d'ITCAM for Applications
ITCAM Monitoring Agent for SAP HANA Database	Informations de référence sur l'ITCAM Monitoring Agent for SAP HANA Database
ITCAM Web Response Time Agent	Knowledge Center d'IBM Tivoli Composite Application Manager pour des transactions

Si des agents coexistants surveillent les mêmes ressources, les scénarios suivants ne sont pas pris en charge :

- Les deux agents stockent des données dans la même instance d'IBM Tivoli Data Warehouse. Par exemple, si les deux agents envoient des données à la même instance de Tivoli Data Warehouse, n'utilisez pas la version 8, 7 ou 6 de l'Agent WebSphere MQ pour surveiller le même gestionnaire de files d'attente sur votre système. Ce scénario s'applique également aux agents à plusieurs instances. Pour plus d'informations, voir «Tivoli Data Warehouse pour le rapport de l'historique», à la page 888.
- Les agents version 6 ou 7 sont intégrés à la Passerelle hybride pour afficher des données issues des deux agents dans la console Cloud APM. Par exemple, si les agents version 6 ou 7 sont connectés à la même instance de serveur Cloud APM via la Passerelle hybride, n'utilisez pas l'agent IBM Integration Bus version 8 ni l'Monitoring Agent for WebSphere Message Broker version 6 ou 7 pour surveiller le même courtier sur votre système.

Si un agent Tivoli Monitoring, intégré à la Passerelle hybride pour afficher les données dans la console Cloud APM, surveille une ressource et que vous voulez que votre agent Cloud APM surveille cette ressource, procédez comme suit :

1. Supprimez l'agent Tivoli Monitoring de toutes les applications qui l'incluent.
2. Supprimez l'agent Tivoli Monitoring du groupe de systèmes gérés Tivoli Monitoring dont l'utilisation a été configurée dans Cloud APM.

3. Attendez au moins 24 heures, puis installez l'agent Cloud APM et ajoutez-le à une application.

Lorsque des agents multi-instances qui coexistent sur le même ordinateur sont intégrés à la Passerelle hybride et surveillent les mêmes ressources, attribuez des noms différents à chaque instance pour afficher les données issues des deux agents dans la console Cloud APM.

Pour les agents dotés d'un collecteur de données, deux agents du même type sont pris en charge. Les données de diagnostic approfondi, de ressource et de suivi des transactions s'affichent dans la console Cloud APM. Les données de ressource s'affichent dans Tivoli Enterprise Portal. Les agents suivants partagent un collecteur de données :

Monitoring Agent for HTTP Server
L'agent HTTP Server est un agent Cloud APM et l'Agent ITCAM pour les serveurs HTTP est un agent IBM Tivoli Monitoring. Si vous disposez des deux agents dans votre environnement, vous pouvez configurer les deux collecteurs de données sur le même serveur HTTP pour les deux agents. Pour plus d'informations sur l'agent HTTP Server, voir «Configuration de la surveillance de HTTP Server», à la page 319.

agent Microsoft .NET
Pour plus d'informations sur la coexistence de l'agent Microsoft .NET, voir «Activation du suivi des transactions dans l'environnement de coexistence d'agent», à la page 490.

Agent WebSphere Applications
Pour plus d'informations sur la coexistence de l'Agent WebSphere Applications, voir «Configuration de l'Agent WebSphere Applications», à la page 793 et «Configuration du collecteur de données pour l'environnement de coexistence d'agent», à la page 794.

Passerelle hybride

Pour afficher les données de surveillance et les événements de vos agents IBM Tivoli Monitoring et OMEGAMON dans la console Cloud APM, vous devez créer un groupe de systèmes gérés et installer la Passerelle hybride d'IBM Cloud Application Performance Management dans votre domaine Tivoli Monitoring, et configurer des communications dans la console Cloud APM Gestionnaire de passerelle hybride.

Consultez les informations de référence pour vous aider à planifier l'installation et la configuration d'une ou plusieurs Passerelles hybrides dans vos environnements Tivoli Monitoring et Cloud APM.

Où installer la Passerelle hybride
Vous pouvez installer la Passerelle hybride dans un ou plusieurs domaines Tivoli Monitoring : un Tivoli Enterprise Monitoring Server concentrateur par domaine. Pour plus d'informations sur l'emplacement d'installation de la Passerelle hybride, voir les informations de la rubrique Préparation de l'installation de la passerelle hybride. Pour connaître la configuration système requise pour la Passerelle hybride qui comprend Tivoli Enterprise Portal Server, voir le site Hybrid Gateway Software Product Compatibility report (onglet **Prerequisites**).

Agents Tivoli Monitoring et OMEGAMON pris en charge
Pour qu'un agent Tivoli Monitoring soit disponible pour la Passerelle hybride, il doit également être pris en charge dans Cloud APM, à l'exception des agents iOS et OMEGAMON. Pour une liste des agents et versions Tivoli Monitoring disponibles, voir Hybrid Gateway supported agents (APM Developer Center).

Si vous avez créé des agents Tivoli Monitoring personnalisés à l'aide d'Agent Builder, vous pouvez ajouter un support pour ces agents à l'environnement Cloud APM. Pour plus d'instructions, voir *Configuration du support des agents personnalisés créés avec Agent Builder* dans le document IBM Agent Builder - Guide d'utilisation.

Pour obtenir la liste des agents OMEGAMON que vous pouvez afficher dans la console Cloud APM, consultez la rubrique d'initiation correspondant à votre édition dans l'ensemble de rubriques relatives à IBM OMEGAMON for Application Performance Management dans IBM Knowledge Center.

Agents Tivoli Monitoring et OMEGAMON dans la console Cloud APM
Après avoir sélectionné l'application prédéfinie «Mes composants» ou une application définie dans le Tableau de bord d'Application Performance qui inclut Tivoli Monitoring ou des systèmes gérés OMEGAMON (ou les deux), un tableau de bord de statut récapitulatif de tous les systèmes gérés s'affiche, ainsi qu'un tableau de bord détaillé d'une instance de système géré unique. Vous pouvez également créer des pages de tableau de bord dans l'onglet Vues personnalisées.

Vous pouvez afficher les événements de situation pour ces agents dans l'onglet Evénements. En revanche, vous ne pouvez pas créer de nouveaux seuils pour les agents Tivoli Monitoring et OMEGAMON dans le gestionnaire de seuils. A la place, créez les nouvelles situations dans Tivoli Monitoring.

Tous les événements Tivoli Monitoring et OMEGAMON possibles ne sont pas disponibles dans le tableau de bord Evénements. Seuls les événements des noeuds d'agent pouvant être ajoutés à une application sont affichés. Par exemple, pour l'agent Tivoli Monitoring for WebSphere Application Server, les événements associés à une instance de serveur particulière sont affichés mais les événements de l'agent dans son ensemble ne le sont pas.

Affichez jusqu'à 1500 systèmes gérés à partir de chaque domaine Tivoli Monitoring
Le nombre maximal de systèmes gérés, sous-noeuds compris, pouvant s'afficher dans un domaine Tivoli Monitoring est de 1500. Par défaut, la limite est de 200 systèmes. Vous pouvez planifier de prendre en charge une plus grande quantité de systèmes. Pour plus d'informations, voir «Planification d'un grand nombre de systèmes gérés», à la page 885.

La limite pour tous les domaines Tivoli Monitoring doit être comprise dans la plage maximale prise en charge par Cloud APM. Pour plus d'informations, voir «Présentation de l'architecture», à la page 32.

Surveillance des ressources uniquement
La surveillance des ressources est disponible pour vos agents Tivoli Monitoring. Pour plus d'informations sur la surveillance des ressources, voir «Offres et modules complémentaires», à la page 35 et «Fonctions», à la page 40. Si vous possédez l'offre IBM Cloud Application Performance Management, Advanced Private, le suivi des transactions et les tableaux de bord de diagnostic ne sont pas disponibles pour les systèmes gérés à partir de votre environnement Tivoli Monitoring.

Tivoli Authorization Policy Server affecte la disponibilité des systèmes gérés par Tivoli Monitoring
Pour les environnements Tivoli Monitoring qui incluent Tivoli Authorization Policy Server, les systèmes gérés disponibles par le biais de la Passerelle hybride sont affectés par les règles d'autorisation. Pour plus d'informations, voir Utilisation des règles d'autorisation par rôle dans Tivoli Monitoring Knowledge Center.

Pour une démonstration vidéo, voir Integrating with Tivoli Monitoring - Passerelle hybride.

Préparation de l'installation de la passerelle hybride

Pour installer la Passerelle hybride d'IBM Cloud Application Performance Management, vous devez d'abord vous assurer que votre environnement est configuré correctement. Examinez les informations pour vous aider à planifier votre installation de la Passerelle hybride.

Où installer la Passerelle hybride

La Passerelle hybride doit être installée sur un système x86-64 Red Hat Enterprise Linux version 6.2 (ou version ultérieure) disposant d'une connexion réseau avec IBM Tivoli Monitoring et IBM Cloud Application Performance Management.

La Passerelle hybride peut être installée sur le même système que Tivoli Enterprise Portal Server ou sur un système distinct de Tivoli Enterprise Portal Server si les systèmes fonctionnent sous Red Hat Enterprise Linux. Toutefois, la Passerelle hybride ne peut pas être installée sur le même système que votre serveur Cloud APM.

Un domaine Tivoli Monitoring comporte un Tivoli Enterprise Monitoring Server concentrateur. Lorsque votre environnement Tivoli Monitoring est constitué de plusieurs domaines, vous pouvez installer la Passerelle hybride dans plusieurs domaines.

Pour la configuration système requise pour la Passerelle hybride, cliquez sur l'onglet **Matériel** dans le Rapport de compatibilité des produits logiciels de la Passerelle hybride.

Configuration du Tivoli Enterprise Portal Server pour la Passerelle hybride

Pour les environnements Tivoli Monitoring où le serveur de portail a une charge lourde, il est recommandé que vous installiez un serveur de portail dédié distinct pour traiter les demandes provenant de la Passerelle hybride. Si vous configurez un serveur de portail distinct :

- Vous pouvez utiliser le même hôte pour le serveur de portail et pour la Passerelle hybride si serveur de portail exécute Red Hat Enterprise Linux.
- Assurez-vous que le serveur de portail distinct dispose du support d'application pour les agents dont les données sont affichées dans la console Cloud APM.
- Assurez-vous que les clients Tivoli Enterprise Portal ne sont pas connectés à un serveur de portail distinct pour effectuer des tâches d'administration telles que la création d'espaces de travail personnalisés, la création de situations et la création de groupes de systèmes gérés.

La version de Tivoli Enterprise Portal Server doit être V6.3 Fix Pack 6 ou supérieure. Si votre serveur de portail est à une version antérieure, les agents Tivoli Monitoring intégrés peuvent ne pas être disponibles pour être ajoutés à une application dans la console Cloud APM.

Le fournisseur de données du tableau de bord IBM Tivoli Monitoring doit être activé sur Tivoli Enterprise Portal Server. Pour plus de détails, voir Verifying the dashboard data provider is enabled dans l'ensemble de rubriques IBM Tivoli Monitoring dans IBM Knowledge Center.

Les ports TCP qui doivent être ouverts sur la Passerelle hybride

Les ports TCP suivants doivent être ouverts sur la Passerelle hybride. Pour chaque port, un côté envoie la demande et l'autre côté fournit une réponse. Le côté qui initie la connexion est indiqué.

- Si vous utilisez HTTP pour communiquer avec le serveur Cloud APM, ouvrez le port 80. Si vous utilisez HTTPS, ouvrez le port 443. La Passerelle hybride initie une connexion unidirectionnelle avec le serveur Cloud APM sur le port 80 ou 443. La communication HTTP est l'option par défaut.

  Si la Passerelle hybride utilise un proxy direct passe-système pour se connecter au serveur Cloud APM, vous pouvez aussi configurer la Passerelle hybride afin que le port du proxy soit utilisé à la place du port 80 ou 443 pour initier les connexions unidirectionnelles avec le serveur Cloud APM. Pour plus d'informations, voir «Utilisation d'un proxy direct pour communiquer avec le serveur Cloud APM», à la page 879.
- Si vous utilisez HTTP pour communiquer avec le serveur de portail, ouvrez le port 15200. Si vous utilisez HTTPS, ouvrez le port 15201. La Passerelle hybride initie une connexion unidirectionnelle avec le serveur de portail sur le port 15200 ou 15201. Pour utiliser un port personnalisé, mettez à jour la valeur du paramètre **Port Portal Server**. Pour plus d'informations, voir «Gestionnaire de Passerelle hybride», à la page 887.

  Si la Passerelle hybride utilise un proxy direct passe-système pour se connecter au serveur de portail, configurez la Passerelle hybride afin que le port du proxy soit utilisé à la place pour les connexions unidirectionnelles qu'il initie avec le serveur de portail. Définissez la valeur du paramètre **Port proxy passe-système**. Pour plus d'informations, voir «Gestionnaire de Passerelle hybride», à la page 887.

- Pour que la Passerelle hybride écoute les événements EIF entrants de Tivoli Enterprise Monitoring Server, ouvrez le port 9998. Le serveur de surveillance initie une connexion unidirectionnelle avec la Passerelle hybride sur le port 9998. La utilitaire d'installation affiche un avertissement si ce port n'est pas ouvert.

Privilèges requis pour exécuter le script d'installation de la Passerelle hybride

Vous devez exécuter le script d'installation de la Passerelle hybride avec les privilèges de superutilisateur. Pour obtenir la liste complète des systèmes d'exploitation pris en charge, visitez le System requirements (APM Developer Center)

Configurez les images de la Passerelle hybride

Avant d'installer la Passerelle hybride, vous devez configurer les images de la Passerelle hybride avec les informations de connexion du serveur Cloud APM. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

Installation de la passerelle hybride

Téléchargez et installez la Passerelle hybride d'IBM Cloud Application Performance Management pour afficher les systèmes gérés à partir de votre domaine IBM Tivoli Monitoring dans la console Cloud APM.

Avant de commencer

Passez en revue et effectuez les tâches de préparation requises dans Préparation de l'installation de la passerelle hybride.

Procédure

Procédez comme suit pour installer la Passerelle hybride dans votre domaine Tivoli Monitoring :

1. Accédez au répertoire dans lequel se trouve votre image de la Passerelle hybride configurée. L'emplacement par défaut sur le serveur Cloud APM est *rép_install*/ccm/depot/. (Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.)
2. Entrez la commande suivante pour extraire les fichiers :

   ```
   tar -xf
   apm_hybrid_gateway_8.1.4.0.tar
   ```

   Le fichier d'archive contient un script utilisé pour déployer la Passerelle hybride. Le script d'installation est extrait dans le répertoire et les fichiers de la Passerelle hybride sont extraits dans des sous-répertoires.
3. Accédez au répertoire de la Passerelle hybride et exécutez le script d'installation avec des privilèges de superutilisateur :

   ```
   cd APM_Hybrid_Gateway_Install_version
   ./install.sh
   ```

   où *version* est la version actuelle, par exemple 8.1.4.0. L'analyse des prérequis de votre environnement commence et prend un moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer l'installation. Vous pouvez également désactiver le prérequis comme indiqué dans Contournement de l'analyse des prérequis.
4. Une fois que le système a été soumis à l'analyse des prérequis, répondez à l'invite pour accepter le contrat de licence en sélectionnant 1 pour oui. Un message vous invite à vous connecter à la console Cloud APM et à configurer la Passerelle hybride avant de continuer. Le nom du profil par défaut, dérivé du nom d'hôte, est affiché également.

5. Appuyez sur Entrée pour accepter le nom par défaut ou entrez un nom de profil. Si vous avez déjà créé un profil pour ce domaine Tivoli Monitoring, utilisez le même nom que celui que vous avez fourni dans le Gestionnaire de la Passerelle hybride. Si vous n'avez pas encore créé un profil, vous pouvez accepter le nom par défaut ou fournir un nouveau nom, mais veillez à en conserver la trace car vous devrez le réutiliser pour créer le profil ultérieurement. (Voir «Configuration de la Passerelle hybride à l'aide de la console Cloud APM», à la page 881.) Une fois que vous avez appuyé sur la touche Entrée, l'installation de la Passerelle hybride continue.

Résultats

La Passerelle hybride est installée dans le répertoire `/opt/ibm/hybridgateway` et démarre automatiquement. Le fichier journal d'installation se trouve dans `/opt/ibm/hybridgateway/logs/install-hybridgateway-`*`horodatage`*`.log`. Les fichiers journaux de la Passerelle hybride se trouvent dans le répertoire `/opt/ibm/wlp/usr/servers/hybridgateway/logs`. Jusqu'à ce que la connexion à Tivoli Enterprise Portal Server soit configurée, les échecs de connexion sont consignés.

Que faire ensuite

- Vous pouvez configurer la Passerelle hybride de sorte à utiliser un proxy direct pour communiquer avec le serveur Cloud APM. Pour plus d'informations, voir «Utilisation d'un proxy direct pour communiquer avec le serveur Cloud APM».
- Vous pouvez vérifier le statut de la Passerelle hybride avec la commande suivante : *`rép_install`*`/hybridgateway/bin/hybridgateway.sh status`. Pour plus d'options, voir «Gestion de la passerelle hybride», à la page 886.
- Si vous n'avez pas encore créé le groupe de systèmes gérés pour la Passerelle hybride, suivez les instructions fournies dans «Création du groupe de systèmes gérés», à la page 880.
- Si vous n'avez pas encore créé un profil de Passerelle hybride pour le domaine Tivoli Monitoring, suivez les instructions dans «Configuration de la Passerelle hybride à l'aide de la console Cloud APM», à la page 881.
- Si votre environnement Tivoli Monitoring comporte un ou plusieurs domaines concentrateur, vous pouvez installer la Passerelle hybride dans d'autres domaines. Répétez les étapes de cette procédure pour installer la Passerelle hybride dans un autre domaine Tivoli Monitoring.

Utilisation d'un proxy direct pour communiquer avec le serveur Cloud APM

Vous pouvez configurer la Passerelle hybride d'IBM Cloud Application Performance Management de sorte à utiliser un proxy direct pour communiquer avec le serveur Cloud APM.

Procédure

1. Sur l'hôte où vous avez installé la Passerelle hybride, éditez le fichier `/opt/ibm/wlp/usr/servers/hybridgateway/bootstrap.properties` :
   - Si la Passerelle hybride utilise le protocole HTTP pour communiquer avec le serveur Cloud APM, ajoutez les lignes suivantes :

     ```
     http.proxyHost=hôte_proxy
     http.proxyPort=hôte_proxy
     ```

   - Si la Passerelle hybride utilise le protocole HTTPS pour communiquer avec le serveur Cloud APM, ajoutez les lignes suivantes :

     ```
     https.proxyHost=hôte_proxy
     https.proxyPort=port_proxy
     ```

   où *hôte_proxy* est le nom d'hôte ou l'adresse IP du proxy, accessible à partir de l'hôte de la Passerelle hybride et *port_proxy* est le port du proxy.
2. Redémarrez l'Passerelle hybride.

Création du groupe de systèmes gérés

Utilisez l'éditeur de groupe d'objet sur le client Tivoli Enterprise Portal pour créer un groupe de systèmes gérés à afficher dans la console Cloud APM.

Avant de commencer

- Les types d'agent IBM Tivoli Monitoring et OMEGAMON que vous pouvez inclure dans le groupe de systèmes gérés doivent faire partie des agents pris en charge. Par exemple, pour Tivoli Monitoring, les agents pris en charge incluent l'Monitoring Agent for Oracle Database ou l'Monitoring Agent for Linux OS.

  Pour obtenir la liste actuelle des agents Tivoli Monitoring pris en charge, visitez le Hybrid Gateway supported agents (APM Developer Center). Pour obtenir la liste des agents OMEGAMON que vous pouvez afficher dans la console Cloud APM, consultez la rubrique d'initiation dans l'ensemble de rubriques relatives à IBM OMEGAMON for Application Performance Management dans IBM Knowledge Center.
- Les agents Tivoli Monitoring et OMEGAMON doivent être connectés à la même infrastructure IBM Tivoli Monitoring. Si votre environnement comporte plusieurs domaines Tivoli Monitoring, créez un groupe de systèmes gérés pour chaque Tivoli Enterprise Monitoring Server concentrateur pour lequel une Passerelle hybride est installée.
- Par défaut, vous pouvez ajouter jusqu'à 200 systèmes gérés au groupe de systèmes gérés pour les afficher à partir du domaine Tivoli Monitoring dans le Tableau de bord d'Application Performance. Vous pouvez augmenter la limite jusqu'à 1500 systèmes en effectuant plusieurs étapes de planification. Pour plus d'informations, voir «Planification d'un grand nombre de systèmes gérés», à la page 885. S'il existe plusieurs Passerelles hybrides pour un environnement Tivoli Monitoring comportant plusieurs concentrateurs, le groupe de systèmes gérés pour chaque domaine doit respecter la limite maximale autorisée par Cloud APM. Pour plus d'informations, voir Architecture overview.
- La méthode par défaut de traitement des sous-noeuds a évolué dans l'édition de Cloud APM version 8.1.4. Dans les éditions précédentes, si vos agents tels que l'Agent WebSphere Applications comportaient des sous-noeuds, vous deviez affecter le noeud de gestion au groupe de systèmes gérés et tous les sous-noeuds étaient inclus automatiquement. Bien qu'un seul noeud de gestion fût affecté au groupe de systèmes gérés, les sous-noeuds étaient inclus dans le comptage visant à déterminer le nombre maximal de systèmes gérés.

  Dans l'édition Cloud APM version 8.1.4 et ultérieure, les sous-noeuds pour lesquels vous souhaitez afficher les données de mesure dans la console Cloud APM doivent être affectés spécifiquement au groupe de systèmes gérés. L'agent de gestion est à présent découvert automatiquement si l'un de ses sous-noeuds est clairement affecté au groupe de systèmes gérés. Pour les applications de surveillance basées sur des sous-noeuds, Cloud APM aura peut-être besoin de demander à l'agent de gestion les informations nécessaires à l'identification précise des ressources de surveillance qui apparaissent dans le navigateur du tableau de bord Cloud APM. C'est pour cette raison qu'avec la version actuelle du mode de reconnaissance, l'agent de gestion est inclus automatiquement et qu'au moins un sous-noeud associé est affecté au groupe de systèmes gérés configuré pour être utilisé par la Passerelle hybride. Le mode de reconnaissance actuel prend en charge le contrôle précis des ressources de sous-noeud pouvant être visualisées dans la console Cloud APM et correspond mieux à la façon dont les applications Cloud APM sont construites, en particulier pour les applications qui impliquent de grands ensembles d'instances de ressource de sous-noeud. Utilisez toujours le mode de reconnaissance par défaut actuel lorsque vous intégrez les agents OMEGAMON à Cloud APM.

  Vous pouvez spécifier la version du mode de reconnaissance utilisée par la Passerelle hybride en affectant la valeur appropriée à une propriété externe appelée `MSN_DISCOVERY_MODE`, traitée par la Passerelle hybride au cours de l'initialisation. Pour contrôler le mode de reconnaissance utilisé par la Passerelle hybride, ajoutez la propriété `MSN_DISCOVERY_MODE` (ou modifiez sa valeur actuelle) au fichier de propriétés suivant sur le système où la Passerelle hybride est installée, puis redémarrez la Passerelle hybride.

  rép_install_PH`/wlp/usr/servers/hybridgateway/bootstrap.properties`

  Les valeurs admises pour la propriété `MSN_DISCOVERY_MODE` sont les suivantes :

– `MSN_DISCOVERY_MODE=1` force la Passerelle hybride à utiliser le mode de reconnaissance d'agent initial, où tous les sous-noeuds sont découverts automatiquement pour n'importe quel agent de gestion affecté au groupe de systèmes gérés Tivoli Monitoring.
– `MSN_DISCOVERY_MODE=2` force la Passerelle hybride à utiliser le nouveau mode de reconnaissance d'agent par défaut où seuls les sous-noeuds clairement affectés au groupe de systèmes gérés sont interrogés par la Passerelle hybride. Le ou les agents de gestion associés sont reconnus automatiquement.

- Si vous préférez créer le groupe de systèmes gérés à l'aide des commandes **`tacmd createsystemlist`** et **`tacmd editsystemlist`** IBM Tivoli Monitoring, voir *IBM Tivoli Monitoring Command Reference* (https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) pour obtenir des informations sur la manière d'exécuter les commandes.

Procédure

Pour créer un groupe de systèmes gérés sur le client Tivoli Enterprise Portal, suivez la procédure ci-dessous.

1. Démarrez le client Tivoli Enterprise Portal avec un ID utilisateur et un mot de passe ayant un accès complet à tous les types de systèmes gérés (Allowed Applications est défini sur All Applications pour l'ID utilisateur.)
2. Cliquez sur **Editeur de groupe d'objets**.
3. Développez l'objet **Système géré** et sélectionnez **Tous les systèmes gérés** pour combiner plusieurs types d'agent (comme Windows et Oracle) dans le groupe de systèmes gérés. Si vous préférez que le groupe de systèmes gérés ne contienne qu'un seul type d'agent de surveillance, tel que système d'exploitation Linux ou applications WebSphere, sélectionnez le type d'agent.
4. Cliquez sur **Créer un groupe** et entrez un nom pour le groupe de systèmes gérés. Le nom peut comporter des lettres et des chiffres, sans espace, ponctuation ni caractère spécial autre que le trait de soulignement (_). Une fois que vous avez cliqué sur **OK**, le nouveau groupe de systèmes gérés s'affiche dans le dossier du système géré.
5. Sélectionnez les systèmes gérés dans la liste **Available Managed Systems** et cliquez sur la pour les déplacer vers la liste **Assigned**. Vous pouvez sélectionner plusieurs systèmes gérés en maintenant la touche Ctrl enfoncée tout en cliquant sur chaque système géré pour les sélectionner. Après avoir sélectionné un système géré, vous pouvez utiliser Maj+clic pour sélectionner tous les systèmes gérés entre cette sélection et la première sélection.
6. Après avoir ajouté des systèmes gérés au groupe, cliquez sur **OK** pour sauvegarder vos modifications et fermer l'éditeur de groupe d'objet.

Que faire ensuite

- Après avoir créé le groupe de systèmes gérés et installé la Passerelle hybride, vous devez configurer cette dernière dans la console Cloud APM.
- Pour la configuration, spécifiez le nom du groupe de systèmes gérés que vous avez créé, l'ID utilisateur Tivoli Enterprise Portal autorisé à accéder à tous les types d'agent et le nom d'hôte et port de Tivoli Enterprise Portal Server.
- Pour obtenir les instructions d'installation, voir «Installation de la passerelle hybride», à la page 878.
- Pour obtenir des instructions de configuration, voir «Configuration de la Passerelle hybride à l'aide de la console Cloud APM».

Configuration de la Passerelle hybride à l'aide de la console Cloud APM

Utilisez la page **Gestionnaire de la passerelle hybride** dans la console Cloud APM afin de configurer la Passerelle hybride d'IBM Cloud Application Performance Management pour la connexion à Tivoli Enterprise Portal Server et la spécification du groupe de systèmes gérés.

Vous pouvez créer un profil de Passerelle hybride pour chaque Tivoli Enterprise Monitoring Server concentrateur de votre environnement.

Procédure

Procédez comme suit pour configurer la Passerelle hybride dans la console Cloud APM.

1. Le cas échéant, connectez-vous à la console Cloud APM. (Voir «Démarrage de la console Cloud APM» , à la page 989.)
2. Cliquez sur **Configuration système** > **Gestionnaire de la Passerelle hybride**. La page s'affiche avec un tableau des Passerelles hybrides configurées pour vos domaines Tivoli Monitoring. Si un profil avec un nom vide est affiché, il s'applique à la Passerelle hybride qui a été installée avant l'édition V8.1.4. Pour plus d'informations, voir «Nom de profil», à la page 887.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre Add Hybrid Gateway, entrez un nouveau nom dans la zone **Nom de profil** et cliquez sur **Ajouter**. Si vous avez déjà installé la Passerelle hybride dans le domaine Tivoli Monitoring, veillez à utiliser le même nom que celui que vous avez indiqué ou accepté au cours de l'installation de la Passerelle hybride. Le nom du profil indiqué au cours de l'installation et le nom que vous entrez ici doivent être une correspondance exacte. La fenêtre Edit Hybrid Gateway s'ouvre.
4. Dans la zone **Nom de groupe de système géré**, entrez le nom du groupe de système géré de la Passerelle hybride. Il s'agit du nom utilisé dans «Création du groupe de systèmes gérés», à la page 880.
5. Indiquez l'adresse, le port et le protocole de communications Web de Tivoli Enterprise Portal Server :

Option	Description
Nom d'hôte Portal Server	Entrez l'adresse IP, le nom d'hôte qualifié complet ou nom de domaine de l'hôte Portal Server.
Port Portal Server	Entrez le numéro de port utilisé par Portal Server pour les communications Web. Le port par défaut est 15200 pour HTTP ou 15201 pour HTTPS. La valeur 0 définit le port 15200 par défaut pour HTTP ou 15201 pour HTTPS.
Protocole Portal Server	Sélectionnez le protocole Internet **HTTP** ou le protocole Internet **HTTPS** sécurisé pour vous connecter à Portal Server.

6. Renseignez les zones **Nom d'utilisateur Portal Server** et **Mot de passe Portal Server** avec le nom d'utilisateur de connexion et le mot de passe correspondant pour démarrer le client Tivoli Enterprise Portal. L'ID utilisateur doit avoir accès à tous les types d'agent de surveillance (Allowed Applications est défini sur All Applications), comme l'ID `sysadmin`. Pour plus d'informations, voir Administrer les utilisateurs dans Tivoli Monitoring IBM Knowledge Center.
7. Si l'accès à Portal Server s'effectue via un serveur proxy, indiquez l'adresse, le port et le protocole Web :

Option	Description
Nom d'hôte proxy passe-système	Entrez l'adresse IP ou le nom qualifié complet du système hôte proxy.
Port proxy passe-système	Entrez le numéro de port du système hôte proxy.
Protocole proxy passe-système	Sélectionnez le protocole utilisé pour les communications via le proxy : HTTP ou HTTPS

Résultats

Une fois que vous cliquez sur **Sauvegarder**, une connexion est établie au service de la Passerelle hybride et les systèmes gérés de votre domaine Tivoli Monitoring sont reconnus. Le groupe de systèmes gérés est interrogé toutes les 5 minutes pour les données de surveillance des ressources.

Que faire ensuite

- Vous devez configurer Tivoli Monitoring pour interagir avec Cloud APM. Pour plus d'informations, voir «Configuration de Tivoli Monitoring pour une intégration à Cloud APM».
- Vous pouvez répéter ces étapes pour ajouter un profil pour chaque domaine Tivoli Monitoring à partir duquel vous souhaitez surveiller des systèmes gérés Cloud APM.
- Vous pouvez gérer les profils existants à l'aide des outils Gestionnaire de la passerelle hybride :

  Sélectionnez une Passerelle hybride et cliquez sur **Editer** pour ouvrir la fenêtre Edit Hybrid Gateway.

  Sélectionnez une Passerelle hybride dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitiez supprimer la Passerelle hybride, le profil est définitivement supprimé.

  Cliquez sur un en-tête de colonne pour trier le tableau en fonction de cette colonne ; utilisez la combinaison Ctrl + Clic sur une autre colonne pour ajouter un tri secondaire.

  Cliquez à l'intérieur de la zone de texte de filtre et entrez le début de la valeur qui va servir au filtrage. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour Arrière.

Configuration de Tivoli Monitoring pour une intégration à Cloud APM

Pour intégrer votre domaine IBM Tivoli Monitoring à Cloud APM, vous devez exécuter des tâches comme la configuration de Tivoli Enterprise Portal Server et de Tivoli Enterprise Monitoring Server concentrateur.

Procédure

Pour chaque domaine Tivoli Monitoring sur lequel une Passerelle hybride est installée, suivez la procédure ci-dessous :

1. Configurez Tivoli Enterprise Portal Server pour activer le fournisseur de données du tableau de bord. Le fournisseur de données doit intégrer Cloud APM à la Passerelle hybride. Pour connaître les instructions, consultez les rubriques suivantes :
   - Windows Windows : Installation du serveur de portail (étape 16c).
   - Linux AIX Configuration du serveur de portail sous Linux ou AIX : procédure de ligne de commande (étape 14).

   Si vous utilisez la fonction de secours automatique, vous devez spécifier une substitution de domaine. La Passerelle hybride utilise le nom de domaine pour collecter les données provenant des deux serveurs de surveillance concentrateurs, quel que soit le concentrateur auquel le serveur de portail est connecté.
2. Si vous souhaitez afficher les événements de situation des agents Tivoli Monitoring dans la console Cloud APM, configurez le serveur de surveillance concentrateur pour l'un des scénarios suivants :
   - Pour envoyer des événements à la Passerelle hybride uniquement.
   - Pour envoyer des événements à la Passerelle hybride et à des récepteurs EIF supplémentaires, tels que des serveurs Netcool/OMNIbus.

   Exécutez l'une des étapes suivantes en fonction de votre scénario applicable.
   a. Pour configurer le Tivoli Enterprise Monitoring Server concentrateur pour qu'il envoie les événements à la Passerelle hybride uniquement, suivez les étapes décrites dans la rubrique Configuring the hub monitoring server to forward events. Indiquez le numéro de port 9998 pour le paramètre **ServerPort**.
      Cloud APM ne transmet pas les événements Tivoli Monitoring à Netcool/OMNIbus. Si vous souhaitez afficher les événements Tivoli Monitoring dans Cloud APM et dans Netcool/OMNIbus, vous devez configurer Tivoli Monitoring pour envoyer les événements aux deux systèmes.

b. Pour configurer le Tivoli Enterprise Monitoring Server concentrateur pour qu'il envoie les événements à la Passerelle hybride et à un autre récepteur EIF, tel qu'un serveur Netcool/OMNIbus, configurez le récepteur EIF par défaut en suivant les étapes décrites dans la rubrique Configuration du serveur de surveillance concentrateur pour le transfert d'événements. La rubrique fournit également des informations sur la création de destinations EIF supplémentaires à l'aide de la commande **tacmd createEventDest**. Indiquez le port 9998 en tant que numéro de port EIF pour la destination de la Passerelle hybride.

c. Configurez toutes les situations qui existent pour les agents du groupe de systèmes gérés de la Passerelle hybride pour vous assurer que les événements de situation sont envoyés à la destination EIF pour la Passerelle hybride. Pour obtenir des instructions, voir la rubrique Spécification des situations qui transmettent des événements Netcool/OMNIbus.

Que faire ensuite

Consultez le Tableau de bord d'Application Performance pour confirmer que les systèmes gérés issus du domaine Tivoli Monitoring sont transmis via la Passerelle hybride :

1. Cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**.
2. Dans la zone récapitulative de «Mes composants», cliquez sur **Composants** pour ouvrir le tableau de bord récapitulatif de statut de tous les systèmes gérés de composant (à l'exception de l'Agent WebSphere Applications). Si vous ne possédez pas d'application «Mes composants», ajoutez une application, comme décrit dans «Gestion des applications», à la page 1145.
3. Recherchez les systèmes gérés issus du domaine Tivoli Monitoring, indiqués par une icône de domaine **ITM** (IBM Tivoli Monitoring) dans le titre du widget de groupe Récapitulatif du statut. Si des systèmes gérés sont manquants, accédez au forum Cloud Application Performance Managementet effectuez une recherche sur «Passerelle hybride».

Vous pouvez créer des applications avec des systèmes gérés provenant des domaines Tivoli Monitoring et inclure des systèmes gérés à partir de votre domaine Cloud APM. Pour plus d'informations, voir «Gestion des applications», à la page 1145.

Configuration du support des agents personnalisés créés avec Agent Builder

Si vous disposez d'agents IBM Tivoli Monitoring personnalisés créés avec Agent Builder, vous pouvez utiliser la nouvelle version d'Agent Builder pour créer des fichiers de support pour Cloud APM. Installez-les ensuite sur le serveur Cloud APM pour afficher des informations issues de votre agent dans la console Cloud APM.

Procédure

1. Si ce n'est pas déjà fait, installez Agent Builder sur n'importe quel ordinateur. Pour plus d'instructions, voir *Installation et démarrage d'Agent Builder* dans le document IBM Agent Builder - Guide d'utilisation.
2. Copiez le sous-répertoire source complet d'Agent Builder dans le répertoire d'espace de travail de votre installation Agent Builder.
3. Démarrez Agent Builder et sélectionnez votre agent dans l'éditeur d'agent. Pour plus d'instructions, voir *Utilisation de l'éditeur d'agent pour modifier l'agent* dans le document IBM Agent Builder - Guide d'utilisation.
4. Cliquez sur le lien Dashboards sur la page de récapitulatif ou dans le panneau de navigation de droite, puis configurez les tableaux de bord et les ressources de Cloud APM. Pour plus d'instructions, voir *Préparation de l'agent pour IBM Cloud Application Performance Management* dans le document IBM Agent Builder - Guide d'utilisation.
5. Créez l'image d'agent dans n'importe quel répertoire. Ne sélectionnez pas **Create a ZIP file** ou **Create a TAR file** . Pour plus d'instructions, voir *Création de l'image d'agent* dans le document IBM Agent Builder - Guide d'utilisation.
6. Dans le répertoire de l'image d'agent, recherchez le fichier `support/`*`code_produit`*`_sda_`*`version`*`.jar`. Copiez ce fichier sur le serveur Cloud APM, dans le répertoire `/opt/ibm/ccm`.

7. Sur le serveur Cloud APM, dans le répertoire /opt/ibm/ccm, exécutez la commande suivante :
   `install_app_support.sh [-force] [-verbose] nom_fichier.jar`

   où *nom_fichier*.jar est le nom du fichier que vous avez copié.

   L'argument -force installe le support pour cet agent même si le support est déjà installé pour la même version ou pour une version plus récente de l'agent.

   L'argument -verbose affiche des messages de progression détaillés.

Résultats

Si vous avez installé la Passerelle hybride et inclus votre agent personnalisé dans le groupe de systèmes gérés pour Cloud APM, la console Cloud APM affiche des informations issues de l'agent dans les 30 minutes .

Planification d'un grand nombre de systèmes gérés

Le nombre maximal de systèmes gérés que vous pouvez voir à partir de votre domaine IBM Tivoli Monitoring est de 1500. Si vous incluez un agent qui a des sous-noeuds dans le groupe de systèmes gérés que vous avez créé pour le profil de Passerelle hybride, tous les sous-noeuds, ainsi que l'agent, sont pris en compte dans la limite. Par défaut, cette limite est de 200 systèmes gérés, mais vous pouvez effectuer un certain nombre d'étapes de planification pour l'étendre.

La limite pour tous les domaines Tivoli Monitoring doit être comprise dans la plage maximale prise en charge par Cloud APM. Pour plus d'informations, voir «Présentation de l'architecture», à la page 32.

- Définissez la valeur de la variable d'environnement Tivoli Enterprise Portal Server **KFW_REPORT_NODE_LIMIT** sur un nombre supérieur ou égal au nombre de systèmes gérés pour la Passerelle hybride. La valeur par défaut est 200. Pour plus d'informations, voir Paramètres de configuration de Tivoli Enterprise Portal Server.
  Si le nombre de systèmes gérés dépasse cette valeur, le journal des messages de Tivoli Enterprise Portal Server KfwServices affiche un message similaire au suivant : `56C6246F.0000-10:ctreportmanager.cpp,2864,"CTReport::Manager::executeDefinitionDual") Query is targeting 1497 nodes which exceeds the current limit of 200 nodes.`
- Si vous visualisez un grand nombre de systèmes, les performances peuvent se dégrader en fonction du type d'agents, du temps d'attente des réseaux entre la Passerelle hybride et les systèmes gérés, et de la taille de l'environnement surveillé par chaque agent (quantité de données collectées et affichées). Pour éviter cet effet, sélectionnez uniquement les agents qui fournissent les données nécessaires et assurent une connectivité réseau rapide entre les systèmes surveillés et l'hôte de Passerelle hybride.
- A mesure que le temps d'attente des réseaux augmente, la durée de collecte des données d'un nombre spécifique d'agents augmente. La Passerelle hybride essaye de regrouper des données de chaque agent toutes les 5 minutes. Si la durée de collecte des données de tous les agents dépasse 5 minutes, la Passerelle hybride manque des échantillons de données, et par conséquent, les mesures ne sont pas disponibles sur les pages du Tableau de bord d'Application Performance.
- Pour compenser les vitesses réseau très lentes, vous pouvez essayer d'augmenter le nombre d'unités d'exécution utilisées par la Passerelle hybride pour recueillir des échantillons de données. Le paramètre **MAX_COLLECTOR_THREADS** du fichier bootstrap.properties de la Passerelle hybride contrôle le nombre d'unités d'exécution. La valeur par défaut est 50.

Désinstallation de la passerelle hybride

Si vous ne voulez plus afficher les systèmes gérés IBM Tivoli Monitoring dans la console Cloud APM, désinstallez la Passerelle hybride d'IBM Cloud Application Performance Management.

Procédure

1. Dans le répertoire *rép_install*/hybridgateway/bin de la Passerelle hybride (comme /opt/ibm/hybridgateway/bin), lancez la commande suivante :
   `./hybridgateway.sh uninstall`

La Passerelle hybride est supprimée et un message confirme qu'elle a été désinstallée avec succès. S'il existe des applications dans la console Cloud APM qui incluent des agents hybrides, ces derniers continuent à apparaître jusqu'à ce que l'infrastructure de surveillance traite leur suppression.

2. Dans la console Cloud APM, cliquez sur **Configuration système** > **Gestionnaire de la Passerelle hybride**.
3. Sélectionnez le profil de la Passerelle hybride dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitiez supprimer la Passerelle hybride, le profil est définitivement supprimé.

Que faire ensuite

- Pour supprimer des systèmes gérés d'agent hybride d'une application dans la console Cloud APM, suivez les instructions décrites dans «Gestion des applications», à la page 1145 pour modifier une application.
- Si au lieu d'avoir confirmation du succès de la suppression du logiciel, vous obtenez un message d'erreur similaire à celui présenté dans cet exemple, consultez le fichier journal pour en connaître les causes possibles :

```
error: Failed dependencies:
ibm-java-x86_64-jre is needed by (installed) smai-kafka-00.08.00.00-1.el6.x86_64
La désinstallation a échoué. Le programme de désinstallation n'est pas parvenu à
supprimer certains composants. Consultez le
 fichier journal
("/tmp/hybridgateway/logs/uninstall-hybridgateway-20150228080551.log") pour plus d'informations.
```

  L'erreur indiquée dans l'exemple s'est produite car ibm-java-x86_64-jre est requis par le package installé en externe sur le système. Le programme d'installation ne supprime pas le JRE car cela rendrait l'autre package inopérant. La solution consiste à désinstaller les produits dépendant d'ibm-java-x86-64-jre avant de désinstaller la Passerelle hybride.

Gestion de la passerelle hybride

Utilisez les commandes disponibles pour la Passerelle hybride d'IBM Cloud Application Performance Management afin de démarrer ou d'arrêter la Passerelle hybride, de vérifier son statut, de la désinstaller et d'en collecter les fichiers journaux si vous y êtes invité par le support IBM.

Pourquoi et quand exécuter cette tâche

Ces étapes considèrent que le répertoire d'installation de la Passerelle hybride est `/opt/ibm/`. Sur le système où la Passerelle hybride est installée, suivez l'une des étapes suivantes à partir de l'invite de commande :

Procédure

- Pour démarrer le service de la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh start**.
- Pour arrêter le service de la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh stop**.
- Pour vérifier le statut du service de la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh status**.
- Pour désinstaller la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh uninstall**. Voir aussi «Désinstallation de la passerelle hybride», à la page 885.
- Pour consulter les fichiers journaux de la Passerelle hybride, accédez à `/opt/ibm/wlp/usr/servers/hybridgateway/logs`.
- Pour collecter les fichiers journaux de la Passerelle hybride pour le support IBM, entrez **/opt/ibm/hybridgateway/collectLogs.sh**. Les fichiers journaux sont collectés et un message affiche l'emplacement des fichiers journaux compressés et vous demande de les retourner au support IBM.

Gestionnaire de Passerelle hybride

Configurez la Passerelle hybride d'IBM Cloud Application Performance Management de sorte qu'elle affiche les données de surveillance de votre domaine IBM Tivoli Monitoring dans la console Cloud APM. Vous pouvez créer un profil de Passerelle hybride pour chaque Tivoli Enterprise Monitoring Server concentrateur de votre environnement.

Une fois que vous avez cliqué sur **Configuration du système** > **Gestionnaire de la Passerelle hybride**, la page est affichée avec une liste des Passerelles hybrides définies.

La page comporte un tableau de toutes les passerelles hybrides configurées pour vos domaines Tivoli Monitoring et contient les outils permettant de gérer les profils de Passerelle hybride :

- **Ajouter** permet d'ouvrir la fenêtre Ajouter une passerelle hybride pour affecter un nom au nouveau profil. Une fois que vous avez entré un nom et cliqué sur **Ajouter**, la fenêtre Editer la passerelle hybride s'ouvre.
- Sélectionnez une passerelle hybride et cliquez sur **Editer** pour ouvrir la fenêtre Editer la passerelle hybride.
- Sélectionnez une passerelle hybride dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitiez supprimer la passerelle hybride, le profil est définitivement supprimé.
- Cliquez sur un en-tête de colonne pour trier le tableau en fonction de cette colonne ; utilisez la combinaison Ctrl + Clic sur une autre colonne pour ajouter un tri secondaire.
- Cliquez à l'intérieur de la zone de texte de filtre et entrez le début de la valeur qui va servir au filtrage. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour Arrière.

Les zones obligatoires que vous devez renseigner pour configurer la Passerelle hybride sont marquées d'un astérisque (*) dans la fenêtre Editer la passerelle hybride.

Nom de profil
Nom attribué à un profil de Passerelle hybride pouvant comporter jusqu'à 128 lettres, chiffres et caractères de soulignement (_).

Le nom de profil est demandé au cours de l'installation de la Passerelle hybride. Si vous avez déjà installé la Passerelle hybride dans le domaine Tivoli Monitoring, utilisez le nom que vous avez indiqué ou accepté au cours de l'installation de la Passerelle hybride.

Les versions plus anciennes de la Passerelle hybride n'utilisent pas un profil nommé pour accéder à leurs données de configuration. Si vous avez installé la Passerelle hybride avant l'édition Cloud APM, Private version 8.1.4, vous disposez d'un nom de profil spécial sans nom (vide). Une seule version plus ancienne de la Passerelle hybride est autorisée à se connecter au serveur Cloud APM. Si vous avez configuré l'ancienne version de la Passerelle hybride, le profil sans nom affiche les valeurs configurées. Dans le cas contraire, le profil sans nom affiche les valeurs par défaut. Vous pouvez conserver le profil sans nom ou le supprimer puis l'ajouter à nouveau ultérieurement le cas échéant. Il peut être utilisé uniquement pour la version 8.1.3 (ou antérieure) de la Passerelle hybride.

Nom de groupe de système géré
Nom du groupe de système géré Tivoli Enterprise Portal Server que vous avez créé pour afficher les agents de surveillance pris en charge dans la console Cloud APM. Tous les types d'agent de surveillance non pris en charge par votre offre Cloud APM n'apparaissent pas dans la console quelle que soit leur inclusion dans le groupe de systèmes gérés.
Pour connaître les instructions et les limitations relatives à la création du groupe de système géré pour l'activation hybride, voir .

Nom d'hôte du serveur de portail
Adresse IP ou nom de domaine complet de l'hôte Tivoli Enterprise Portal Server.

Port Portal Server
Numéro de port utilisé par Tivoli Enterprise Portal Server pour les communications. Le port par défaut est `15200` pour HTTP ou `15201` pour HTTPS. La valeur 0 définit le port `15200` par défaut pour HTTP ou `15201` pour HTTPS.

Protocole Portal Server
Détermine si le protocole HTTP Internet ou le protocole HTTPS sécurisé doit être utilisé pour se connecter à Tivoli Enterprise Portal Server. Valeur par défaut : `http`.

Nom d'utilisateur Portal Server
Nom d'utilisateur pour démarrer le client Tivoli Enterprise Portal. Cet ID utilisateur doit avoir accès à tous les types d'agent de surveillance (Allowed Applications est défini sur All Applications). Pour plus d'informations, voir Administrer les utilisateurs dans Tivoli Monitoring Knowledge Center.)

Mot de passe utilisateur Portal Server
Mot de passe associé au nom d'utilisateur de la connexion à Tivoli Enterprise Portal.

Nom d'hôte proxy passe-système
Utilisé si Tivoli Enterprise Portal Server communique via un serveur proxy passe-système. Entrez l'adresse IP ou le nom qualifié complet du système hôte proxy.

Port proxy passe-système
Utilisé si Tivoli Enterprise Portal Server communique via un serveur proxy passe-système. Entrez le numéro de port pour la communication avec le proxy.

Protocole proxy passe-système
Utilisé si Tivoli Enterprise Portal Server communique via un serveur proxy passe-système. Entrez le protocole utilisé pour les communications via le proxy. Valeur par défaut : `http`.

Les agents Tivoli Monitoring que vous affichez dans la console Cloud APM se trouvent dans votre environnement IBM Tivoli Monitoring. Vous pouvez les afficher dans les pages du Tableau de bord d'Application Performance, mais vous ne pouvez pas créer de seuils pour ces agents dans le Gestionnaire de seuils.

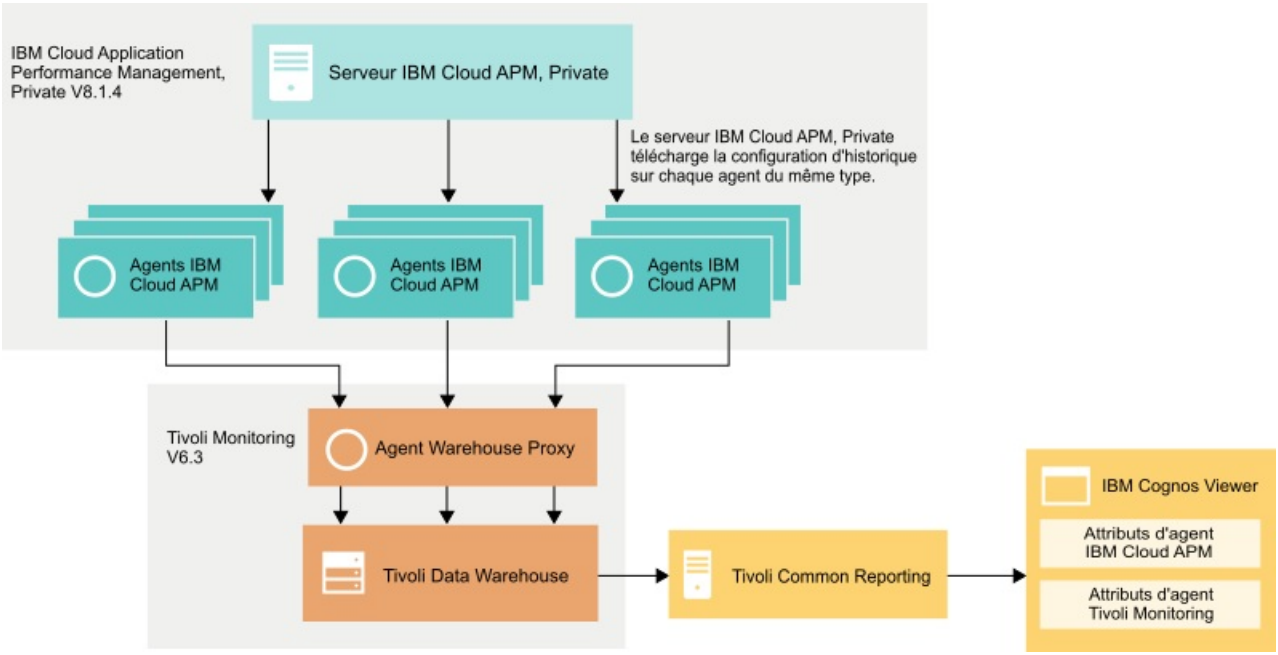
Tivoli Data Warehouse pour le rapport de l'historique

Si votre environnement géré inclut un domaine IBM Tivoli Monitoring avec Tivoli Data Warehouse, vous pouvez envoyer des échantillons de données à l'entrepôt de données à partir des agents Cloud APM. Vous pouvez ensuite accéder aux données pour générer des rapports Cognos dans Tivoli Common Reporting.

Par exemple, si vous disposez d'agents Windows OS dans vos domaines Tivoli Monitoring et Cloud APM, vous pouvez générer un rapport Windows OS de données d'historique issues des deux domaines.

Pour permettre l'envoi des données historiques à Tivoli Data Warehouse, vous devez effectuer la configuration pour chaque type d'agent. Vous configurez l'adresse de l'agent Warehouse Proxy, les ensembles de données à partir desquels recueillir des échantillons, la fréquence de collecte des données, et la durée de conservation des données localement.

Cette configuration est stockée sur le serveur Cloud APM. Le serveur répartit les informations de configuration entre les agents. Les agents envoient des données historiques à l'agent Warehouse Proxy, qui les stocke dans Tivoli Data Warehouse.



Dans votre environnement IBM Cloud Application Performance Management, les données d'historique peuvent être visualisées jusqu'à 24 heures et être comparées jusqu'à 7 jours dans les tableaux de bord avec les graphiques et les tableaux d'historique, comme décrit dans «Ajustement et comparaison de mesures dans le temps», à la page 1138. Si vous disposez également d'un environnement IBM Tivoli Monitoring, vous pouvez stocker les données d'historique issues des agents Cloud APM à long terme dans Tivoli Data Warehouse. Les données peuvent ensuite être extraites de l'entrepôt de données pour générer des rapports avec Tivoli Common Reporting et d'autres applications.

Pour chaque agent qui peut envoyer des données d'historique à Tivoli Data Warehouse, vous pouvez rechercher un fichier de configuration d'historique d'échantillon sur votre serveur Cloud APM. Pour configurer des agents de ce type afin d'envoyer des données à Tivoli Data Warehouse, créez une copie de ce fichier, modifiez-la pour fournir les informations de configuration nécessaires et sauvegardez-la sur le serveur.

Agents Cloud APM admissibles à la collecte des données d'historique

L'intégration de Tivoli Data Warehouse est disponible uniquement pour les agents qui existent aussi dans Tivoli Monitoring. Seuls les ensembles de données (groupes d'attributs) qui sont également disponibles dans Tivoli Monitoring peuvent être envoyés à Tivoli Data Warehouse.

Les agents suivants sont admissibles :

- Monitoring Agent for Cisco UCS (v6)
- Monitoring Agent for Citrix Virtual Desktop Infrastructure (vd)
- Monitoring Agent for DataPower (bn)
- Monitoring Agent for Db2 (ud)
- Monitoring Agent for HMC Base (ph)
- Monitoring Agent for IBM Integration Bus (qi)
- Monitoring Agent for Linux KVM (v1)
- Monitoring Agent for Linux OS (lz)
- Monitoring Agent for Microsoft Active Directory (3z)
- Monitoring Agent for Microsoft Cluster Server (q5)
- Monitoring Agent for Microsoft Exchange Server (ex)

- Monitoring Agent for Microsoft Hyper-V Server (hv)
- Monitoring Agent for Microsoft Internet Information Services (q7)
- Monitoring Agent for Skype for Business Server (ql)
- Monitoring Agent for Microsoft SharePoint Server (qp)
- Monitoring Agent for Microsoft SQL Server (oq)
- Monitoring Agent for Oracle Database (rz)
- Monitoring Agent for SAP Applications (sa)
- Monitoring Agent for UNIX OS (ux)
- Monitoring Agent for VMware VI (vm)
- Monitoring Agent for WebSphere Applications (yn)
- Monitoring Agent for WebSphere MQ (mq)
- Monitoring Agent for Windows OS (nt)

Configuration de la collecte des données d'historique pour les agents Performance Management

Les exemples de fichiers d'historique pour les agents sont disponibles sur votre serveur Cloud APM. Utilisez le modèle de fichier pour votre agent comme base pour créer le fichier xml de configuration d'historique sur le serveur Cloud APM. Ce serveur propage la configuration à tous les agents de ce type.

Le fichier historique spécifie l'adresse de l'agent Warehouse Proxy, les ensembles de données à partir desquels collecter les modèles, la fréquence de collecte des données et la durée de conservation des données en local.

Avant de commencer

Avant de configurer un agent Cloud APM pour envoyer des données à Tivoli Data Warehouse, assurez-vous que l'agent Tivoli Monitoring équivalent est installé dans votre environnement Tivoli Monitoring. Sinon, les fonctions de génération de rapports peuvent échouer.

Pourquoi et quand exécuter cette tâche

Pour chaque agent qui peut envoyer des données d'historique à Tivoli Data Warehouse, vous pouvez rechercher un fichier de configuration d'historique d'échantillon sur votre serveur Cloud APM. Créez votre fichier de configuration en copiant le fichier échantillon et en éditant la copie.

Le fichier inclut les ensembles de données (groupes d'attributs) de l'agent qui peut envoyer des données d'historique à Tivoli Data Warehouse. Si un ensemble de données particulier n'existe pas dans le modèle de fichier, il est probable que cet ensemble de données n'existe également pas dans le produit d'agent Tivoli Monitoring version 6.3 ou qu'il n'est pas disponible pour la collecte des données d'historique. Vous pouvez supprimer certains ensembles de données si vous ne voulez pas collecter de données pour eux.

Le fichier contient également d'autres paramètres d'échantillon ou par défaut. Vous devez modifier ces paramètres pour configurer la collecte des données d'historique.

Ne modifiez pas le fichier de configuration d'historique d'échantillon, parce que la mise à jour suivante du serveur Cloud APM peut l'écraser. Au lieu de cela, créez-en une copie.

Procédure

1. Localisez le fichier *nom_produit*_sample_history.xml sur le système du serveur Cloud APM :
   rép_install/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source/*cp*

où *rép_install* est /opt/ibm ou le répertoire spécifié au cours de l'installation du serveur et *cp* est le code produit à deux caractères. Les codes produit apparaissent entre parenthèses après le nom du produit dans les «Agents Cloud APM admissibles à la collecte des données d'historique», à la page 889.

2. Créez une copie du fichier *nom_produit*_sample_history.xml dans le même répertoire avec le nom suivant :

   *cp*_history.xml

   où *cp* est le code produit à deux caractères. Par exemple, ud_history.xml pour l'agent Db2 et lz_history.xml pour l'agent du système d'exploitation Linux.

   Conseil : Un fichier avec le nom *cp*_history.xml existe déjà par défaut à l'emplacement. Vous pouvez écraser ce fichier avec votre nouveau fichier de configuration.
3. Ouvrez *cp*_history.xml dans un éditeur de texte.
4. Indiquez l'emplacement de l'agent Warehouse Proxy. La valeur par défaut est :

   <WAREHOUSE LOCATION="ip.pipe:*#adresseréseau*[*port#*]"/>

   Modifiez les parties suivantes de cette valeur :

   ip.pipe:
   Pour la communication RPC non sécurisée entre l'agent et l'agent Warehouse Proxy, conservez ip.pipe:. Pour la communication RPC non sécurisée, remplacez par ip.spipe:.

   Avertissement : En raison des problèmes de compatibilité de certificat, la communication sécurisée (ip.spipe) entre les agents Cloud APM et l'agent Warehouse Proxy nécessite une configuration supplémentaire importante. Pour obtenir des instructions, voir «Configuration des communications sécurisées pour la collecte des données d'historique», à la page 894. Si vous voulez activer l'intégration à Tivoli Data Warehouse sans procédures de configuration supplémentaires, utilisez le paramètre ip.pipe non sécurisé.

   #adresseréseau
   Définissez l'adresse IP ou le nom de système hôte qualifié complet du système où l'agent Warehouse Proxy est installé. Tous les hôtes où vos agents Cloud APM s'exécutent doivent pouvoir établir une connexion sortante directe au système à l'aide de cette adresse ou de ce nom d'hôte.

   Avertissement : Si vous utilisez une adresse IP, ajoutez le signe # avant l'adresse. Si vous utilisez un nom de système hôte qualifié complet, assurez-vous que le signe # n'est pas présent avant le nom d'hôte.

   port# Entrez le port d'écoute de l'agent Warehouse Proxy. Le port par défaut est 63358 pour le protocole ip.pipe et 65100 pour le protocole ip.spipe.

   Conseil : Vous pouvez rechercher la valeur de la chaîne d'emplacement d'entrepôt dans le fichier journal RAS1 sur l'hôte d'agent Warehouse Proxy. Le fichier journal RAS1 est situé dans le répertoire *Rép_install*/logs. Le format de nom de fichier est hostname_hd_*horodatage* - *nbre*.log (par exemple, *myhost01_hd_56d4db3c-01.log*). Recherchez dans le fichier journal le message register_interface.

   Un message de journal RAS1 peut ressembler à ceci :

   "register_interface") Registering "Candle_Warehouse_Proxy": ip.pipe:#9.48.147.34[63358]

   Dans cet exemple, définissez la valeur suivante dans le fichier :

   <WAREHOUSE LOCATION="ip.pipe:#9.48.147.34[63358]"/>
5. Si vous voulez indiquer plusieurs destinations ou protocoles, séparez chacun par un point-virgule (;). Par exemple, vous pouvez définir la valeur :

   ```
   <WAREHOUSE LOCATION=
   "ip.spipe:#9.11.123.45[65100];ip.pipe:#9.11.123.45[63358];ip.pipe:tdw.example.com[63358]"/>
   ```

Dans ce cas, lorsqu'un agent démarre des communications avec l'agent Warehouse Proxy, il essaye la communication RPC sécurisée, puis revient à la communication RPC non sécurisée.

6. Facultatif : Supprimez les lignes HISTORY EXPORT des ensembles de données à partir desquels vous ne voulez pas collecter l'historique :

   ```
   <HISTORY EXPORT=«60» INTERVAL=«15» RETAIN=«6» TABLE=«NOMTABLE»/>
   ```

   où *NOMTABLE* est le nom de l'ensemble de données. Par exemple, pour ne pas envoyer d'échantillons de données Linux_IP_Address à Tivoli Data Warehouse, supprimez la ligne `<HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="Linux_IP_Address"/>`. Les ensembles de données sont décrits dans la section «Attributs» de l'aide sur l'agent et du PDF de référence.

7. Dans les lignes restantes, spécifiez l'intervalle d'exportation des données, l'intervalle de collecte des données et la durée de conservation des échantillons collectés en local :

   EXPORT Ce paramètre indique l'intervalle en minutes d'exportation des données d'historique vers Tivoli Data Warehouse. Les intervalles d'exportation admis sont 15, 30 et des valeurs divisibles par 60 : un intervalle supérieur à 60 peut être 120, 180, 240, etc., jusqu'à 1440. L'intervalle d'exportation doit également être divisible par la valeur du paramètre **INTERVAL**. Si vous saisissez une valeur non valide, aucune donnée d'historique n'est collectée et exportée pour l'ensemble de données spécifié. Valeur par défaut : 60 minutes.

   INTERVAL
   Ce paramètre indique l'intervalle de collecte de données d'historique en minutes. L'intervalle de collecte minimal est de 1 et l'intervalle maximal est de 1440 (24 heures). Les intervalles valides doivent être des diviseurs de 60 ou être divisibles par 60 : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, et 30 ; un intervalle supérieur à 60 pourrait être 120, 180, 240, etc., jusqu'à 1440. Si vous saisissez une valeur non valide, aucun historique n'est collecté pour l'ensemble de données spécifié. Valeur par défaut : 15.

   RETAIN Ce paramètre définit la durée de conservation des données d'historique à court terme en heures, avec un minimum de 1 heure. Il n'existe aucune autre limite que celle imposée par l'espace de stockage sur le système. Une fois que la durée de conservation a été atteinte, l'agent supprime les échantillons de données les plus anciens lorsque de nouveaux échantillons arrivent. Cette durée de conservation garantit que si l'agent perd la communication avec Tivoli Data Warehouse pendant quelque temps, les données d'historique ne sont pas perdues. Valeur par défaut : 6 heures.

8. Sauvegardez le fichier *cp*`_history.xml`.
9. Répétez ces étapes pour chaque agent que vous voulez configurer pour la collecte des données d'historique.

Résultats

Après avoir sauvegardé le fichier *cp*`_history.xml`, le serveur Cloud APM traite le fichier et répartit la configuration entre tous les agents en ligne du même type. Le délai de réception et de traitement du fichier, puis de lancement de la collecte des données d'historique par l'agent dépend des conditions de charge de travail du serveur. Cela peut prendre 15 minutes ou plus dans certains cas. Lorsque de nouveaux agents du type applicable arrivent en ligne, le serveur répartit automatiquement la configuration entre eux.

Une fois que vos agents ont reçu la configuration, ils continuent d'envoyer des données d'historique à Tivoli Data Warehouse même si la connexion au serveur Cloud APM est perturbée.

Exemple

L'exemple suivant est le contenu du fichier de configuration `ud_history.xml` pour l'Agent Db2. Avec cette configuration, l'agent collecte des échantillons des attributs `KUDINFO00` toutes les 15 minutes, transmet les

données collectées toutes les heures à l'agent Warehouse Proxy à l'adresse IP 9.88.765.432, port 63358, et conserve les données collectées localement pendant 6 heures :

```
<PRIVATECONFIGURATION>
  <WAREHOUSE LOCATION="ip.pipe:#9.88.765.432[63358]"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KUDINFO00"/>
</PRIVATECONFIGURATION>
```

Voici le fichier historique d'échantillon `linux_os_sample_history.xml` pour l'agent du système d'exploitation Linux :

```
<PRIVATECONFIGURATION>
  <WAREHOUSE LOCATION="ip.pipe:#netaddress[port#]"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ_CPU"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ_DISK"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ_VM_STATS"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ_NETWORK"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ_SYSTEM_STATISTICS"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="Linux_IP_Address"/>
</PRIVATECONFIGURATION>
```

Le fichier de configuration d'historique `lz_history.xml` que vous créez à partir de l'échantillon peut ressembler à ce qui suit :

```
<PRIVATECONFIGURATION>
  <WAREHOUSE LOCATION=
"ip.spipe:#9.11.123.45[65100];ip.pipe:#9.11.123.45[63358];ip.pipe:tdw.example.com[63358]"/>
  <HISTORY EXPORT="60" INTERVAL="15" RETAIN="6" TABLE="KLZ_CPU"/>
  <HISTORY EXPORT="240" INTERVAL="60" RETAIN="24" TABLE="KLZ_DISK"/>
  <HISTORY EXPORT="120" INTERVAL="15" RETAIN="6" TABLE="KLZ_SYSTEM_STATISTICS"/>
</PRIVATECONFIGURATION>
```

Désactivation et réactivation des protocoles de communication de données d'historique pour un hôte d'agent

Par défaut, tous les agents installés peuvent utiliser tous les protocoles RPC de communication qui sont configurés pour le type d'agent afin d'envoyer des données à l'agent Warehouse Proxy. La configuration d'entreposage de l'historique d'un agent peut inclure des protocoles de communication IP.PIPE et IP.SPIPE. Vous pouvez désactiver l'un des protocoles sur un hôte d'agent individuel.

Normalement, cette action n'est pas nécessaire.

Pourquoi et quand exécuter cette tâche

Si vous souhaitez désactiver un protocole de communication de données d'historique pour un hôte particulier où l'agent est installé, ou réactiver un protocole sur un hôte d'agent où il a été désactivé, procédez comme ci-après sur l'hôte de l'agent.

Important : Ce paramètre est valable uniquement pour la communication entre l'agent et l'agent de Warehouse Proxy. Il n'a aucune incidence sur la communication entre l'agent et le serveur Cloud APM.

Procédure

1. Accédez au répertoire suivant :
   - Windows *rép_install*\BIN, par défaut, C:\IBM\APM\BIN
   - Linux *rép_install*/bin, par défaut, /opt/ibm/apm/bin
   - AIX *rép_install*/bin, par défaut, /opt/ibm/apm/bin
2. Exécutez la commande suivante :
   - Windows `enableprotocols.bat pipe=`*yes*`|`*no* `spipe=`*yes*`|`*no*
   - Linux AIX `./enableprotocols.sh pipe=`*yes*`|`*no* `spipe=`*yes*`|`*no*

   Où *yes*|*no* est yes pour activer un protocole ou no pour le désactiver.

Par exemple, pour activer IP.SPIPE et désactiver IP.PIPE sur un système Windows, exécutez la commande :

```
enableprotocols.bat pipe=no spipe=yes
```

Conseil : Exécutez la commande `enableprotocols` sans paramètres pour savoir quels protocoles sont actuellement activés et désactivés.

Configuration des communications sécurisées pour la collecte des données d'historique

Si vous voulez utiliser des communications sécurisées (IP.SPIPE) entre les agents Cloud APM et l'agent Tivoli Monitoring Warehouse Proxy, vous devez effectuer des étapes de configuration supplémentaires sur l'agent Cloud APM, sur l'agent Warehouse Proxy, sur tous les agents Cloud APM devant utiliser des communications sécurisées pour des données d'historique, et éventuellement sur d'autres composants de Tivoli Monitoring.

Pour pouvoir communiquer via le protocole de communication sécurisée (IP.SPIPE), les deux côtés doivent posséder chacun des certificats correspondants qui utilisent le même type de chiffrement.

Chaque côté doit présenter un certificat à l'autre côté. L'autre côté doit identifier la signature d'une autorité de certification sur ce certificat. Pour identifier la signature, ce côté doit détenir un certificat racine de l'autorité de certification.

Par exemple, le côté A doit avoir son propre certificat ainsi que le certificat de l'autorité de certification racine correspondant au certificat du côté B. Le côté B, à son tour, doit avoir son propre certificat ainsi que le certificat de l'autorité de certification racine correspondant au côté A. (Les deux côtés peuvent également avoir le même certificat et le même certificat de l'autorité de certification racine, mais ce n'est pas une obligation.)

Cependant, en raison des différentes configurations par défaut de Tivoli Monitoring et de Cloud APM, les types de chiffrement de certificat ne correspondent pas. Lorsque l'infrastructure de Cloud APM est installée, elle est configurée pour utiliser les certificats numériques (ECDSA) TLS1.2 Elliptic Curve. Or l'infrastructure de Tivoli Monitoring, y compris les agents Warehouse Proxy, est configurée pour utiliser des certificats RSA.

Important : La communication non sécurisée (IP.PIPE) n'est pas affectée par ce problème. Vous pouvez utiliser la communication IP.PIPE entre tous les composants sans configuration supplémentaire.

Important : Une instance installée d'un composant peut utiliser des certificats ECDSA et des certificats RSA pour les communications. Elle ne peut pas utiliser de certificats ECDSA pour communiquer avec un composant ni de certificats RSA pour communiquer avec un autre composant.

Pour activer la communication sécurisée entre les agents Cloud APM et l'agent Warehouse Proxy, vous devez effectuer au minimum les opérations suivantes :

- Installez un ou plusieurs agents Tivoli Monitoring Warehouse Proxy. Ces agents doivent communiquer avec des agents Cloud APM, et non avec des agents Tivoli Monitoring.
- Générez un nouveau certificat numérique ECDSA. Signez-le avec une autorité de certification autosignée ou obtenez-le signé par une autorité de certification tierce de votre choix. Ce certificat est utilisé sur certains composants de Tivoli Monitoring.
- Extrayez les certificats de l'autorité de certification ECDSA que les agents Cloud APM utilisent.
- Sur les agents Warehouse Proxy, installez le nouveau certificat ainsi que le certificat de l'autorité de certification correspondant aux agents.
- Sur tous les agents Cloud APM devant utiliser des communications sécurisées avec l'agent Warehouse Proxy, installez le certificat racine de l'autorité de certification qui a signé le nouveau certificat (soit l'autorité de certification autosignée, soit l'autorité de certification tierce).

A l'issue de ces étapes, les agents Warehouse Proxy ne pourront pas communiquer avec le serveur Tivoli Enterprise Monitoring Server via un protocole sécurisé, car le serveur de surveillance possède des certificats RSA.

Vous pouvez utiliser la communication non sécurisée (IP.PIPE) entre les agents Warehouse Proxy et le serveur de surveillance. Par exemple, vous pouvez déployer un serveur de surveillance distant séparé sur le même hôte que les agents Warehouse Proxy, et utiliser IP.PIPE pour connecter les agents proxy au serveur de surveillance sur l'`hôte local`. De cette façon, toutes les communications réseau restent sécurisées.

Vous pouvez également installer le nouveau certificat ECDSA sur le serveur Tivoli Enterprise Monitoring Server. Dans ce cas toutefois, tous les autres composants de Tivoli Monitoring (agents de surveillance compris) se connectant à ce serveur via SPIPE doivent également être reconfigurés pour ce certificat, de même que tous les composants se connectant à ces composants via SPIPE et ainsi de suite.

Vous pouvez à tout moment utiliser une communication non sécurisée (PIPE) pour associer la partie de votre infrastructure utilisant des certificats ECDSA à la partie utilisant des certificats RSA. En l'absence de communications non sécurisées, vous devez installer le nouveau certificat sur la totalité de votre infrastructure Tivoli Monitoring.

Création et signature du nouveau certificat :

Vous devez créer un certificat ECDSA et utiliser soit une autorité de certification autosignée, soit une autorité de certification tierce pour le signer.

Pourquoi et quand exécuter cette tâche

Le certificat doit également être signé. Vous pouvez créer une autorité de certification autosignée sur le même hôte afin de signer le certificat. Sinon, vous pouvez soumettre le certificat à une autorité de certification tierce de votre choix (dans votre organisation ou ailleurs) pour signature. Dans ce cas, il vous faut obtenir le certificat racine de cette autorité de certification.

Procédure

1. Connectez-vous à n'importe quel hôte où les agents Cloud APM sont installés.

   Important : Ces instructions reposent sur les postulats suivants :
   - L'hôte exécute le système d'exploitation Linux. Dans le cas d'un système Windows ou AIX, modifiez les chemins d'accès et les commandes.
   - Les agents sont installés dans le chemin d'accès par défaut (`/opt/ibm/apm/agent`). Si vous utilisez un chemin personnalisé, remplacez le chemin par défaut par le chemin personnalisé.
2. Créez un répertoire de travail pour tous les fichiers de clés que vous allez créer. Affectez à la variable d'environnement `KEYFILES_DIR` le chemin d'accès complet à ce répertoire. Par exemple :

   ```
   mkdir -v -p ~/itm_keystore
   export KEYFILES_DIR=~/itm_keystore
   ```

   Conseil : Vous devrez installer ces fichiers de clés sur certains composants Tivoli Monitoring ultérieurement. Pour cette raison, ces fichiers de clés sont connus sous le nom de *fichiers de clés d'ITM* et le certificat que vous créez, sous le nom de *certificat d'ITM*.
3. Configurez l'hôte pour l'utilisation des outils GSKit. Les outils se trouvent dans le répertoire `/opt/ibm/apm/agent/lx8266/gs`. Apportez les modifications suivantes aux variables d'environnement à l'aide de l'interpréteur de commandes :

   ```
   export GSK_HOME=/opt/ibm/apm/agent/lx8266/gs
   export PATH=$GSK_HOME/bin:$PATH
   export LD_LIBRARY_PATH=$GSK_HOME/lib64:$LD_LIBRARY_PATH
   ```

Important : Dans cet exemple, `lx8266` est le code de plateforme correspondant à un système Linux 64 bits. Si vous utilisez un autre système d'exploitation, modifiez le code de plateforme en fonction du produit, de la plateforme et des codes composant IBM Tivoli.

Important : Les instructions à venir utilisent la commande `gsk8capicmd_64`. Sur une plateforme 32 bits, le nom de la commande est `gsk8capicmd`.

4. Facultatif : Si vous n'utilisez pas d'autorité de certification tierce, créez votre propre autorité de certification.

   Conseil : Comme cette autorité de certification signe le certificat ITM, elle est connue sous le nom d'*autorité de certification racine d'ITM*. Ce n'est pas la même autorité de certification que celle utilisée pour votre environnement Tivoli Monitoring existant.

   a. Choisissez un mot de passe pour le nouveau magasin de clés de l'autorité de certification. Ce mot de passe chiffre la clé privée de l'autorité de certification et le magasin de clés. Affectez-le à la variable d'environnement `ROOTCAPASS`. Par exemple :

      ```
      export ROOTCAPASS="votre_motdepasse_autoritédecertification_racine_ITM"
      ```

   b. Créez un sous-répertoire pour y stocker les clés de la nouvelle autorité de certification sous le répertoire keyfiles que vous avez créé :

      ```
      mkdir -v -p ${KEYFILES_DIR}/apmCA
      mkdir -v -p ${KEYFILES_DIR}/apmCA/keyfiles
      mkdir -v -p ${KEYFILES_DIR}/apmCA/exports
      ```

   c. Créez le magasin de clés de l'autorité de certification racine d'ITM :

      ```
      gsk8capicmd_64 -keydb -create -db ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -pw
      $ROOTCAPASS -expire 3650 -fips -stash
      ```

   d. Créez le certificat de l'autorité de certification racine d'ITM :

      ```
      gsk8capicmd_64 -cert -create -db ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -stashed
      -label ITM_Root_CA_Certificate -ca true -size 256 -dn
      "CN=ITM_Root_CA,O=my_corp,OU=my_div" -default_cert yes -expire 3695 -sigalg
      EC_ecdsa_with_SHA256 -fips
      ```

      Conseil : L'option `-dn` fournit un nom distinctif pour votre certificat. Vous pouvez modifier ce nom en lui affectant les valeurs appropriées pour votre environnement :

      - Remplacez `CN=ITM_Root_CA` par un autre identificateur, par exemple, `CN=Example_ITM_CA`
      - Remplacez `O=my_corp` par le nom de votre société, par exemple, `CN=Example_Co`
      - Remplacez `OU=my_div` par le nom de votre division, par exemple, `CN=Example_Div`

      Avertissement : Vous pouvez également modifier le nom `-label ITM_Root_CA_Certificate`, à condition de modifier aussi toutes les commandes suivantes pour être en adéquation avec le nouveau nom de l'étiquette. Sinon, les communications sécurisées risquent d'échouer.

   e. Faites du certificat de l'autorité de certification racine d'ITM le certificat par défaut dans le nouveau magasin de clés :

      ```
      gsk8capicmd_64 -cert -setdefault -db ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -stashed
      -label ITM_Root_CA_Certificate -fips
      ```

      Avertissement : Si vous avez modifié l'option `-label` à l'étape 4d, vous devez affecter le même nom au paramètre `-label` dans cette commande et dans toutes les commandes suivantes.

   f. Exportez le nouveau certificat de l'autorité de certification racine d'ITM de manière à pouvoir l'importer dans d'autres magasins de clés :

      ```
      gsk8capicmd_64 -cert -extract -target ${KEYFILES_DIR}/apmCA/exports/apmCA.cer -db
      ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -stashed -label ITM_Root_CA_Certificate -fips
      ```

   g. Facultatif : Pour afficher le certificat de l'autorité de certification racine d'ITM que vous avez créé dans le magasin de clés de l'autorité de certification racine d'ITM, utilisez les commandes suivantes.

- Affichez les noms de tous les certificats trouvés dans le magasin de clés de l'autorité de certification racine :

  ```
  gsk8capicmd_64 -cert -list -db ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -stashed
  ```

- Affichez les détails d'un certificat particulier dans le magasin de clés de l'autorité de certification racine d'ITM :

  ```
  gsk8capicmd_64 -cert -details -showOID -label "ITM_Root_CA_Certificate" -db
  ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -stashed
  ```

A ce stade, la nouvelle autorité de certification racine d'ITM est créée dans le répertoire `"${KEYFILES_DIR}"/apmCA`. Ce répertoire contient deux sous-répertoires : `keyfiles` et `exports`. Le sous-répertoire `keyfiles` contient le magasin de clés de l'autorité de certification racine, tandis que le sous-répertoire `exports` contient le certificat public de l'autorité de certification racine.

5. Utilisez les outils GSKit pour créer un nouveau certificat numérique et une demande de signature de certificat (CSR).

   Ce certificat doit être utilisé par les composants de Tivoli Monitoring (au minimum, les agents Warehouse Proxy). Ce certificat est connu sous le nom de *certificat d'ITM*.

   Le certificat est identifié par un nom d'hôte. Ce nom d'hôte n'a pas besoin de correspondre à un vrai hôte. Les instructions de cette rubrique utilisent le nom d'hôte `default.itm`. Vous pouvez en choisir un autre si vous le souhaitez.

   a. Choisissez un mot de passe pour le nouveau magasin de clés d'ITM. Le mot de passe chiffre la clé privée et le magasin de clés d'ITM. Affectez-le à la variable d'environnement `ITMPASS`. Par exemple :

      ```
      export ITMPASS="votre_motdepasse_ITM"
      ```

   b. Créez le sous-répertoire pour y stocker les clés d'ITM sous le répertoire keyfiles que vous avez créé :

      ```
      mkdir -v -p ${KEYFILES_DIR}/default.itm
      mkdir -v -p ${KEYFILES_DIR}/default.itm/keyfiles
      mkdir -v -p ${KEYFILES_DIR}/default.itm/exports
      ```

   c. Créez le magasin de clés d'ITM :

      ```
      gsk8capicmd_64 -keydb -create -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb -pw
      $ITMPASS -expire 3650 -fips -stash
      ```

   d. Importez la clé publique de l'autorité de certification racine dans le magasin de clés d'ITM. Si vous utilisez une autorité de certification autosignée, importez l'autorité de certification racine d'ITM qui a été créée et exportée à l'étape 4, à la page 896. Pour ce faire, utilisez la commande suivante :

      ```
      gsk8capicmd_64 -cert -add -file ${KEYFILES_DIR}/apmCA/exports/apmCA.cer -trust enable
      -label ITM_Root_CA_Certificate -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb
      -stashed -fips
      ```

      Avertissement : Si vous avez modifié la valeur de l'option `-label` dans votre certificat de l'autorité de certification racine d'ITM, affectez le même nom à l'option `-label` dans cette commande.

      Si vous utilisez une autorité de certification tierce, vous devez posséder un certificat racine issu de cette autorité de certification. Utilisez le nom de fichier de ce certificat au lieu de `${KEYFILES_DIR}/apmCA/exports/apmCA.cer`, de même que l'étiquette fournie par l'autorité de certification dans l'option `-label`.

   e. Créez le nouveau certificat numérique et la demande de signature de certificat (CSR) correspondante :

      ```
      gsk8capicmd_64 -certreq -create -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb
      -stashed -label IBM_Tivoli_Monitoring_Certificate -size 256 -file ${KEYFILES_DIR}/
      default.itm/keyfiles/default.itmReq.arm -dn "CN=ITM_Hostname,O=my_corp,OU=my_div" -sigalg
      EC_ecdsa_with_SHA256 -fips
      ```

Conseil : L'option `-dn` fournit un nom distinctif pour votre certificat. Vous pouvez modifier ce nom en lui affectant les valeurs appropriées pour votre environnement :

- Remplacez `CN=ITM_Hostname` par un autre identificateur, par exemple, `CN=Example_ITM_Hostname`
- Remplacez `O=my_corp` par le nom de votre société, par exemple, `O=Example_Co`
- Remplacez `OU=my_div` par le nom de votre division, par exemple, `OU=Example_Div`

Avertissement : Vous pouvez également modifier le nom `-label IBM_Tivoli_Monitoring_Certificate`. Dans ce cas, vous devrez aussi modifier tous les composants de Tivoli Monitoring (au minimum, les agents Warehouse Proxy) pour utiliser cette étiquette. Pour plus d'informations, voir «Configuration des composants de Tivoli Monitoring avec le nouveau certificat», à la page 901. Vous devrez également modifier toutes les commandes suivantes afin d'être en phase avec le nouveau nom d'étiquette. Sinon, les communications sécurisées risquent d'échouer.

6. Signez le certificat. Selon l'autorité de certification utilisée :
   - Avec une autorité de certification autosignée, exécutez la commande suivante :

     ```
     gsk8capicmd_64 -cert -sign -db ${KEYFILES_DIR}/apmCA/keyfiles/keyfile.kdb -stashed -expire
     3650 -label ITM_Root_CA_Certificate -file ${KEYFILES_DIR}/default.itm/keyfiles/
     default.itmReq.arm -target ${KEYFILES_DIR}/default.itm/keyfiles/default.itmSigned.arm
     ```

     Avertissement : Si vous avez modifié la valeur de l'option `-label` dans votre certificat de l'autorité de certification racine d'ITM, affectez le même nom à l'option `-label` dans cette commande.
   - Avec une autorité de certification tierce, envoyez le fichier `${KEYFILES_DIR}/default.itm/keyfiles/default.itmReq.arm` à l'autorité de certification, puis attendez de recevoir le certificat signé. Sauvegardez le certificat signé sous `${KEYFILES_DIR}/default.itm/keyfiles/default.itmSigned.arm`.
7. Recevez le certificat nouvellement signé dans le magasin de clés d'ITM :

   ```
   gsk8capicmd_64 -cert -receive -file ${KEYFILES_DIR}/default.itm/keyfiles/
   default.itmSigned.arm -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb -stashed -fips
   ```
8. Faites du certificat nouvellement signé le certificat par défaut pour le magasin de clés d'ITM.

   ```
   gsk8capicmd_64 -cert -setdefault -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb
   -stashed -label IBM_Tivoli_Monitoring_Certificate -fips
   ```

   Avertissement : Si vous avez modifié la valeur de l'option `-label` dans votre certificat d'ITM, affectez le même nom à l'option `-label` dans cette commande.

Extraction et importation de certificats d'autorité de certification d'agent :

Vous devez créer une copie du répertoire keyfiles que vos agents Cloud APM utilisent, puis utiliser cette copie pour extraire les certificats de l'autorité de certification. Importez ces certificats de l'autorité de certification dans le magasin de clés d'ITM.

Avant de commencer

Effectuez toutes les opérations indiquées dans la rubrique «Création et signature du nouveau certificat», à la page 895. En particulier, si vous utilisez une autorité de certification tierce, attendez de recevoir le certificat signé et rangez-le dans le magasin de clés.

Pourquoi et quand exécuter cette tâche

Le magasin de clés de vos agents Cloud APM contient les certificats de l'autorité de certification qu'ils utilisent. Pour activer les communications sécurisées, vous devez effectuer les actions suivantes :

- Déterminez le certificat par défaut des agents.
- Déterminez le certificat qui a signé le certificat par défaut.
- Vérifiez si ce certificat est un certificat racine.

- Si ce certificat n'est pas un certificat racine, déterminez quel certificat l'a signé. Si ce certificat n'est pas non plus un certificat racine, déterminez quel certificat l'a signé, et ce jusqu'à ce que vous trouviez le certificat racine.
- Extrayez la clé publique pour chaque certificat de signataire (pas seulement le certificat racine).
- Importez chaque clé publique dans le magasin de clés d'ITM.

Plus tard, vous devrez modifier le magasin de clés des agents Cloud APM (voir «Modification du magasin de clés pour des agents Cloud APM», à la page 902), c'est pourquoi vous devez vous assurer que la copie du répertoire keyfiles demeure disponible.

Exécutez cette procédure sur l'hôte que vous avez utilisé pour la procédure «Création et signature du nouveau certificat», à la page 895. Les agents Cloud APM doivent être installés sur cet hôte.

Avertissement : Vous pourriez avoir des agents Cloud APM qui se connectent à des serveurs Cloud APM différents. Par exemple, vous pourriez avoir différents serveurs locaux, différents abonnements à l'offre Cloud APM, ou différents agents qui se connectent aux serveurs locaux et cloud. De tels agents possèdent des certificats de l'autorité de certification qui leurs sont propres. Dans ce cas, vous devez créer une copie des magasins de clés pour chacun de ces types d'agent, puis extraire les certificats d'autorité de certification à partir de chacune des copies.

Procédure

1. Copiez les fichiers de clés d'agent Cloud APM dans un répertoire de travail :

   ```
   mkdir -v -p ~/apm_agent_keystore/keyfiles
   cp /opt/ibm/apm/agent/keyfiles/* ~/apm_agent_keystore/keyfiles
   ```

   Avertissement : Si vous avez des agents Cloud APM qui se connectent à des serveurs Cloud APM différents, vous devez également obtenir une copie du répertoire `keyfiles` auprès d'un hôte d'agent pour chaque serveur et placer celle-ci dans un répertoire de travail distinct sur l'hôte où vous effectuez la configuration. Par exemple, `~/apm_agent_onprem1_keystore/keyfiles`, `~/apm_agent_cloud1_keystore/keyfiles`, et ainsi de suite.
2. Définissez la variable d'environnement `APM_AGENT_KEYFILES_DIR` de sorte qu'elle pointe sur le répertoire de travail keyfiles d'agent spécifique que vous avez créé, par exemple :

   ```
   export APM_AGENT_KEYFILES_DIR=~/apm_onprem_keystore
   ```
3. Emettez la commande certificate list afin de contrôler les noms de certificat dans le magasin de clés d'agent :

   ```
   gsk8capicmd_64 -cert -list -db ${APM_AGENT_KEYFILES_DIR}/keyfiles/keyfile.kdb -stashed
   ```

   Examinez la sortie de la commande et recherchez le nom du certificat par défaut, signalé par le signe `*`. Par exemple, la sortie pourrait être la suivante :

   ```
    Certificates found
   * default, - personal, ! trusted, # secret key
   !       apmCA
   !       server_key
   *-      IBM_Tivoli_Monitoring_Certificate
   ```

   Dans cet exemple, le nom du certificat par défaut est `IBM_Tivoli_Monitoring_Certificate`.

   Conseil : Les agents Cloud APM peuvent utiliser les mots «Tivoli Monitoring» dans les noms de certificat. Cette situation est normale.
4. Pour examiner le certificat par défaut, utilisez la commande certificate details, par exemple :

   ```
   gsk8capicmd_64 -cert -details -db ${APM_AGENT_KEYFILES_DIR}/keyfiles/keyfile.kdb -stashed
   -label "IBM_Tivoli_Monitoring_Certificate"
   ```

   Utilisez l'étiquette du certificat par défaut dans l'option `-label`. Mettez l'étiquette entre guillemets.
5. Examinez la première partie du résultat de la commande, par exemple :

```
Label : IBM_Tivoli_Monitoring_Certificate
Key Size : 256
Version : X509 V3
Serial : 0a5936d9a7b572cb
Issuer : CN=APM_MIN_server
Subject : CN=default.agent
```

Comparez le contenu des zones `Issuer` et `Subject`. Ces zones sont les mêmes pour un certificat racine. En principe, le certificat par défaut n'est pas le certificat racine. (Si le contenu des zones `Issuer` et `Subject` du certificat par défaut est identique, contactez le support IBM.)

6. Utilisez la zone `Issuer` pour déterminer le certificat de signataire de ce certificat. La zone contient un *nom de certificat de signataire* qui est soit l'étiquette, soit la valeur de la zone `Subject` du certificat de signataire.

   Examinez la liste affichée à l'étape 3, à la page 899. Effectuez l'une des opérations suivantes :

   - Si vous trouvez le nom du certificat de signataire dans la liste des étiquettes, examinez le certificat de signataire.
   - Si la liste ne contient pas le nom du certificat de signataire, examinez tous les autres certificats dans la liste jusqu'à ce que vous en trouviez un dont la zone `Subject` corresponde au nom du certificat de signataire.

   Pour examiner un certificat, utilisez la commande suivante :

   ```
   gsk8capicmd_64 -cert -details -db ${APM_AGENT_KEYFILES_DIR}/keyfiles/keyfile.kdb -stashed
   -label "étiquette"
   ```

   Affectez à l'option `-label` l'étiquette du certificat que vous examinez. Placez l'étiquette entre guillemets.

   Dans cet exemple, la liste ne contient pas le nom du certificat de signataire. Commençons par la première étiquette indiquée dans la liste, `apmCA` :

   ```
   gsk8capicmd_64 -cert -details -db ${APM_AGENT_KEYFILES_DIR}/keyfiles/keyfile.kdb -stashed
   -label "apmCA"
   ```

   La sortie est la suivante :

   ```
   Label : apmCA
   Key Size : 256
   Version : X509 V3
   Serial : 5b023cefbbf4076e
   Issuer : CN=APM_MIN_server
   Subject : CN=APM_MIN_server
   ```

   Puisque la valeur de la zone `Subject` correspond au nom du certificat de signataire, il s'agit du certificat correct.

7. Extrayez le certificat de signataire que vous avez identifié à l'étape 6 :

   ```
   gsk8capicmd_64 -cert -extract -target ${KEYFILES_DIR}/default.itm/exports/apm_agentCA.cer
   -db ${APM_AGENT_KEYFILES_DIR}/keyfiles/keyfile.kdb -stashed -label "apmCA"
   ```

   Affectez à l'option `-label` l'étiquette du certificat de signataire. Mettez l'étiquette entre guillemets.

8. Importez le fichier certificat extrait dans le magasin de clés d'ITM.

   ```
   gsk8capicmd_64 -cert -add -file ${KEYFILES_DIR}/default.itm/exports/apm_agentCA.cer -trust
   enable -label "apmCA" -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb -stashed
   ```

   Affectez à l'option `-label` l'étiquette du certificat de signataire. Mettez l'étiquette entre guillemets.

9. Dans les informations sur le certificat de signataire que vous avez affichées à l'étape 6, comparez les valeurs des zones `Issuer` et `Subject`. Si elles sont identiques, il s'agit du certificat racine. Passez à l'étape suivante. Si les valeurs diffèrent, vous devez rechercher le certificat de signataire de ce certificat. Le nom du certificat de signataire est indiqué dans la zone `Issuer`. Répétez la procédure, en commençant par l'étape 6, pour rechercher le certificat de signataire et le traiter.

Important : Vous devez extraire chaque certificat de signataire que vous trouvez, y compris le certificat racine, et l'ajouter au magasin de clés d'ITM.

Dans cet exemple, les zones `Issuer` et `Subject` du certificat `apmCA` correspondent. Il s'agit donc du certificat racine.

10. Si vous avez des agents Cloud APM qui se connectent à des serveurs Cloud APM différents, répétez la procédure en commençant par l'étape 2, à la page 899 pour le magasin de clés de l'agent, sur chacun de ces serveurs.
11. Facultatif : Pour afficher les certificats que vous avez ajoutés au magasin de clés d'ITM, utilisez les commandes suivantes :
    - Pour afficher les noms de tous les certificats du magasin de clés d'ITM :

      ```
      gsk8capicmd_64 -cert -list -db ${KEYFILES_DIR}/default.itm/keyfiles/keyfile.kdb -stashed
      ```
    - Pour examiner les détails d'un certificat particulier dans le magasin de clés d'ITM :

      ```
      gsk8capicmd_64 -cert -details -label "label" -db ${KEYFILES_DIR}/default.itm/keyfiles/
      keyfile.kdb -stashed
      ```

      Affectez à l'option `-label` l'étiquette du certificat que vous examinez. Mettez l'étiquette entre guillemets.

Configuration des composants de Tivoli Monitoring avec le nouveau certificat :

Vous devez configurer certains composants de Tivoli Monitoring pour qu'ils utilisent le nouveau certificat d'ITM. Au minimum, il vous faut effectuer cette configuration pour les agents Warehouse Proxy.

Avant de commencer

Vous devez déterminer les composants de Tivoli Monitoring devant utiliser le nouveau certificat et les installer. Les règles suivantes s'appliquent :

- Les agents Tivoli Monitoring Warehouse Proxy qui utilisent une communication sécurisée avec des agents Cloud APM doivent utiliser le nouveau certificat.
- Les composants qui utilisent le nouveau certificat ne peuvent pas utiliser la communication (SPIPE) sécurisée avec les composants qui n'utilisent pas le nouveau certificat, car ce dernier utilise le chiffrement ECDSA, alors que les certificats Tivoli Monitoring existants utilisent le chiffrement RSA. Ils peuvent toujours utiliser la communication (PIPE) non sécurisée avec n'importe quel composant.
- Les composants installés dans le même emplacement d'installation utilisent le même certificat. Vous pouvez toutefois installer des composants dans divers emplacements sur le même hôte. Ces composants peuvent utiliser des certificats différents.

Pour éviter d'avoir à installer le nouveau certificat sur une grande partie de votre infrastructure, installez les nouveaux agents Warehouse Proxy qui reçoivent des données d'historique des agents Cloud APM et non des agents Tivoli Monitoring. Configurez-les Warehouse Proxy de sorte qu'ils puissent utiliser le nouveau certificat. Utilisez le protocole de communication (IP.PIPE) non sécurisée pour connecter ces agents Warehouse Proxy à un serveur Tivoli Enterprise Monitoring Server.

Si vous devez garantir que toutes les connexions réseau sont sécurisées, vous pouvez installer un serveur Tivoli Enterprise Monitoring Server distant sur chaque hôte où sont installés les nouveaux agents Warehouse Proxy. Utilisez des emplacements d'installation différents pour les agents Warehouse Proxy et pour le serveur de surveillance. Ne configurez **pas** le serveur de surveillance pour l'utilisation du nouveau certificat. Configurez la communication IP.PIPE sur l'hôte local entre les agents Warehouse Proxy et le serveur de surveillance. Dans ce cas, le serveur de surveillance peut utiliser des certificats existants pour communiquer avec le reste de l'infrastructure Tivoli Monitoring.

Vous pouvez aussi utiliser le nouveau certificat pour communiquer entre les agents Warehouse Proxy et un serveur de surveillance. Dans ce cas, toutefois, vous pourriez avoir besoin de déployer le nouveau

certificat vers une grande partie de votre infrastructure Tivoli Monitoring. Cette solution peut comporter beaucoup d'opérations manuelles.

Pourquoi et quand exécuter cette tâche

Exécutez la procédure suivante sur les agents Tivoli Monitoring Warehouse Proxy qui communiquent avec les agents Cloud APM. Si votre planification l'exige, vous pouvez également exécuter la procédure sur tous les autres composants de Tivoli Monitoring.

Procédure

1. Connectez-vous à l'hôte où est installé le composant de Tivoli Monitoring.
2. Accédez au répertoire d'installation du composant.
3. Sauvegardez le sous-répertoire `keyfiles`.
4. Copiez les fichiers du magasin de clés d'ITM que vous avez créés (`${KEYFILES_DIR}/default.itm/keyfiles` sur l'hôte où vous avez créé le magasin de clés, voir «Création et signature du nouveau certificat», à la page 895) dans le sous-répertoire `keyfiles` en écrasant tous les fichiers existants.
5. Copiez le fichier `KAES256.ser` de la sauvegarde que vous avez créée à l'étape 3 dans le sous-répertoire `keyfiles`.
6. Définissez les variables de configuration Tivoli Monitoring suivantes. Pour des instructions sur la définition des variables de configuration, voir Edition des paramètres de configuration de votre environnement. Si certaines variables ne figurent pas dans la liste, créez-les.
   a. Redéfinissez la variable `KDEBE_FIPS_MODE_ENABLED` sur `SuiteB-128`.
   b. Redéfinissez la variable `ITM_AUTHENTICATE_SERVER_CERTIFICATE` sur `Y`.
   c. Redéfinissez la variable `ITM_AUTHENTICATE_CLIENT_CERTIFICATE` sur `Y`.
   d. Si vous avez utilisé une valeur personnalisée pour l'étiquette du nouveau certificat d'ITM, vous devez configurer le composant de Tivoli Monitoring pour qu'il utilise la nouvelle étiquette. L'étiquette par défaut fournie dans les instructions est `IBM_Tivoli_Monitoring_Certificate`. Les composants sont déjà configurés pour l'utiliser.

      Si vous souhaitez une étiquette personnalisée, redéfinissez la variable `KDEBE_KEY_LABEL` sur l'étiquette.

Modification du magasin de clés pour des agents Cloud APM :

Vous devez importer le certificat de l'autorité de certification de votre nouveau certificat d'ITM dans le magasin de clés pour les agents Cloud APM. Il vous faut également déployer le nouveau magasin de clés sur chaque hôte d'agent devant utiliser des communications sécurisées pour envoyer les données d'historique.

Pourquoi et quand exécuter cette tâche

Dans une étape précédente, «Extraction et importation de certificats d'autorité de certification d'agent», à la page 898, vous avez créé une copie du magasin de clés d'agent Cloud APM.

Vous devez importer le certificat de l'autorité de certification pour votre nouveau certificat d'ITM dans cette copie. Vous avez créé et signé ce certificat dans «Création et signature du nouveau certificat», à la page 895.

Si vous avez créé une autorité de certification d'ITM autosignée, importez le certificat de l'autorité de certification racine d'ITM que vous avez créée. Si une autorité de certification tierce a signé le certificat, importez le certificat racine fourni par cette dernière. Ensuite, déployez le nouveau magasin de clés sur chaque agent Cloud APM devant utiliser des communications sécurisées avec un agent Tivoli Monitoring Warehouse Proxy.

Avertissement : Si des agents Cloud APM se connectent à des serveurs Cloud APM différents, répétez cette procédure sur chacun des serveurs. Modifiez chaque magasin de clés et déployez les nouveaux magasins de clés sur les agents. Veillez à déployer chaque magasin de clés sur les agents appropriés. Si vous copiez un magasin de clés pour des agents utilisant un serveur Cloud APM dans un hôte d'agent qui se connecte à un autre serveur Cloud APM, l'agent cesse de communiquer avec le serveur.

Procédure

1. Affectez à la variable d'environnement `APM_AGENT_KEYFILES_DIR` le chemin d'accès complet du répertoire de travail avec une copie des magasins de clés d'agent, par exemple :

   ```
   export APM_AGENT_KEYFILES_DIR="~/apm_agent_keystore/keyfiles"
   ```

2. Importez la clé publique de l'autorité de certification dans le magasin de clés d'agent. Si vous avez fait appel à une autorité de certification d'ITM autosignée, utilisez le certificat de l'autorité de certification racine d'ITM que vous avez créée. Pour ce faire, utilisez la commande suivante :

   ```
   gsk8capicmd_64 -cert -add -file ${KEYFILES_DIR}/apmCA/exports/apmCA.cer -trust enable
   -label ITM_Root_CA_Certificate -db ${APM_AGENT_KEYFILES_DIR}/keyfiles/keyfile.kdb -stashed
   ```

   Vérifiez que la valeur de l'option `-label` est identique à celle utilisée pour le certificat de l'autorité de certification racine d'ITM.

   Si une autorité de certification tierce a signé le certificat, remplacez `${KEYFILES_DIR}/apmCA/exports/apmCA.cer` par le chemin et le nom du fichier contenant le certificat racine fourni par cette autorité de certification. Utilisez l'étiquette fournie par l'autorité de certification dans l'option `-label`.

3. Sur chaque hôte où les agents Cloud APM sont installés et doivent utiliser des communications sécurisées pour envoyer les données d'historique, sauvegardez le contenu du répertoire *rép_install_agent*`/keyfiles`.
4. Copiez les fichiers du répertoire `${APM_AGENT_KEYFILES_DIR}/keyfiles` dans le répertoire *rép_install_agent*`/keyfiles` sur chaque hôte où les agents Cloud APM sont installés et doivent utiliser des communications sécurisées pour envoyer les données d'historique. Ecrasez les fichiers existants du même nom. Ne supprimez pas les fichiers qui ne sont pas remplacés par les nouveaux fichiers.
5. Conservez la copie de travail du magasin de clés. Si vous prévoyez d'installer des agents Cloud APM, vous pouvez copier les nouveaux fichiers du magasin de clés sur les hôtes d'agent afin d'activer les communications sécurisées pour les données d'historique.

Fichiers de clés et variables d'environnement :

Les deux composants de Tivoli Monitoring et de Cloud APM utilisent le composant GSKit pour gérer les communications sécurisées à l'aide de certificats. Ils stockent les certificats dans un répertoire et requièrent certaines variables de configuration.

Fichiers du magasin de clés de certificats

Les composants de Tivoli Monitoring et de Cloud APM stockent leurs clés secrètes et leurs certificats dans le répertoire *rép_intall_de_base*`/keyfiles`. Ce répertoire est partagé entre tous les composants installés dans le même chemin d'accès. Il contient les fichiers suivants :

keyfile.kdb
: Base de données de certificats de clés par défaut. Le certificat nommé IBM_Tivoli_Monitoring_Certificate est utilisé pour la négociation par défaut.

keyfile.sth
: Fichier de dissimulation qui contient le mot de passe brouillé pour la base de données de clés. Assurez-vous que les droits sur ce fichier sont verrouillés pour que seuls les identificateurs d'utilisateurs d'agent et les administrateurs puissent les lire.

keyfile.crl
: Fichier hérité concernant le stockage des listes de révocation de certification. Obsolète.

keyfile.jks
Version Java du fichier de clés keyfile.kdb. Fichier présent dans les composants de Cloud APM.

server.jks
Ce fichier est présent seulement sur les installations de serveur de Cloud APM et est utilisé par le serveur. Il s'agit de la version Java du fichier de clés `keyfiles/default.server/keyfiles/keyfile.kdb`. Le nom de répertoire `default.server` est utilisé lorsque le serveur Cloud APM est installé.

KAES256.ser
Clé AES 256 bits utilisée pour chiffrer localement les données de configuration chiffrées ou pour déchiffrer les accréditations transmises par le biais des fonctions de déploiement distantes. Cette clé n'est pas utilisée pour le chiffrement des communications.

Variables de configuration

Les deux composants de Tivoli Monitoring et de Cloud APM utilisent des variables de configuration pour gérer les connexions sécurisées. En ce qui concerne les composants de Tivoli Monitoring, vous pouvez utiliser l'utilitaire Manage Tivoli Enterprise Monitoring Services pour modifier les variables. Les composants de Cloud APM stockent les variables dans des fichiers de configuration.

KEYFILE_DIR
Répertoire du fichier de clés où la base de données de clés est stockée.

Valeur par défaut : *rép_install_de_base*`/keyfiles`

KDEBE_KEYRING_FILE
Fichier base de données des certificats de clés.

Valeur par défaut : *rép_install_de_base*`/keyfiles/keyfile.kdb`

KDEBE_KEYRING_STASH
Fichier de dissimulation qui contient le mot de passe brouillé pour la base de données de clés.

Valeur par défaut : *rép_install_de_base*`/keyfiles/keyfile.sth`

KDEBE_KEY_LABEL
Etiquette du certificat spécifique à utiliser pour l'authentification. Un certificat doit être présent même lorsqu'aucune validation n'est activée.

Valeur par défaut : `IBM_Tivoli_Monitoring_Certificate`

Les variables suivantes indiquent la façon dont les certificats sont traités :

KDEBE_FIPS_MODE_ENABLED
Mode d'exploitation de conformité FIPS.

Valeur par défaut (Cloud APM) : `SuiteB-128`

Valeur par défaut (Tivoli Monitoring) : non définie.

ITM_AUTHENTICATE_SERVER_CERTIFICATE
Si la valeur de ce paramètre est Y, le serveur recevant l'appel doit présenter un certificat signé valide au client, sinon la connexion ne sera pas établie.

Valeur par défaut (Cloud APM) : `Y`

Valeur par défaut (Tivoli Monitoring) : `N`

ITM_AUTHENTICATE_CLIENT_CERTIFICATE
Si la valeur de ce paramètre est Y, le serveur effectuant l'appel doit présenter un certificat signé valide au serveur, sinon la connexion ne sera pas établie.

Valeur par défaut (Cloud APM) : `Y`

Valeur par défaut (Tivoli Monitoring) : `N`

Intégration à OMEGAMON

Vous pouvez afficher les données et les événements de vos composants d'application OMEGAMON dans la console Cloud APM en achetant OMEGAMON for APM et en utilisant la Passerelle hybride pour connecter un ou plusieurs agents OMEGAMON déployés à Cloud APM.

Avant de commencer

- Pour utiliser OMEGAMON for APM, vous devez disposer soit de l'offre IBM Cloud Application Performance Management, Advanced, soit de l'offre IBM Cloud Application Performance Management, Base.
- Un ou plusieurs agents sous licence OMEGAMON doivent s'exécuter sur les partitions logiques z Systems en cours de surveillance.
- Les agents OMEGAMON sont connectés à l'infrastructure IBM Tivoli Monitoring.

Pour obtenir la liste des agents OMEGAMON que vous pouvez afficher dans la console Cloud APM, consultez la rubrique d'initiation correspondant à votre édition dans l'ensemble de rubriques relatives à IBM OMEGAMON for Application Performance Management dans IBM Knowledge Center.

Procédure

Pour intégrer OMEGAMON à Cloud APM, procédez comme suit :

1. Installez OMEGAMON for APM. Pour plus de détails, reportez-vous aux rubriques d'installation dans la collection de rubriques IBM OMEGAMON for Application Performance Management, sur l'IBM Knowledge Center. Une fois qu'OMEGAMON for APM est installé, effectuez les tâches de Passerelle hybride suivantes :
   a. Installez l'Passerelle hybride.
   b. Créez le groupe de systèmes gérés que vous voulez afficher dans la console Cloud APM.
   c. Configurez la Passerelle hybride dans la console Cloud APM de sorte à pouvoir connecter la Passerelle hybride à Tivoli Enterprise Portal Server et spécifiez un groupe de systèmes gérés.

   Pour plus d'informations, voir les rubriques associées à la section «Passerelle hybride», à la page 875.
2. Pour afficher le statut de vos applications dans le tableau de bord, connectez-vous à la console Cloud APM à partir de votre navigateur. Pour plus d'informations, voir «Démarrage de la console Cloud APM», à la page 989.

Intégration à Netcool/OMNIbus

Vous pouvez réacheminer les événements de IBM Cloud Application Performance Management vers votre gestionnaire d'événements IBM Tivoli Netcool/OMNIbus sur site.

Procédure

1. Configurez l'intégration pour Netcool/OMNIbus.
2. Une fois que vous avez configuré l'intégration à Netcool/OMNIbus, vous pouvez personnaliser la manière dont les événements de seuil sont mappés aux événements transmis.

Configuration de l'intégration pour Netcool/OMNIbus

Après avoir installé l' serveur Cloud APM, vous devez copier les règles d'événement vers Probe for Tivoli EIF et les modifier. Vous devez également mettre à jour Netcool/OMNIbus ObjectServer et le schéma de base de données.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez installé le serveur Cloud APM, les fichiers de configuration suivants se trouvent dans le répertoire *rép_install*/ccm/omnibus (*rép_install* représentant le répertoire /opt/IBM/ ou C:\IBM\ par défaut ou le répertoire que vous avez spécifié lors de l'installation du serveur Cloud APM) :

- itm_apm_db_update.sql
- itm_event.rules
- itm_apm_event.rules

Important : Procédez comme suit même si vos systèmes ObjectServer Probe for Tivoli EIF et Netcool/OMNIbus sont déjà intégrés à IBM Tivoli Monitoring, à Probe for Tivoli EIF, à IBM SmartCloud Monitoring - Application Insight, à IBM SmartCloud Application Performance Management ou à une version précédente de Cloud APM.

Procédure

Dans cette procédure, lorsque vous suivez les liens vers la documentation d'IBM Tivoli Monitoring, exécutez uniquement les étapes fournies sur la page liée.

1. Copiez les fichiers itm_event.rules et itm_apm_event.rules dans le répertoire d'installation de Probe for Tivoli EIF.

   Linux *rép_install*/tivoli/netcool/omnibus/probes/linux2x86

   Windows *rép_install*\Tivoli\Netcool\omnibus\probes\win32

   Où *rép_install* est le répertoire /opt/IBM/ ou C:\IBM\ par défaut ou le répertoire que vous avez spécifié lors de l'installation du serveur Cloud APM.
2. Ouvrez le fichier Probe for Tivoli EIF tivoli_eif.rules dans un éditeur de texte et effectuez l'une des étapes suivantes :
   - Si vous êtes un client IBM Tivoli Monitoring existant et que vous avez déjà terminé l'intégration d'OMNIbus, ajoutez cette ligne à votre fichier itm_event.rules : include "itm_apm_event.rules".
   - Si vous n'avez pas encore configuré l'intégration d'OMNIbus, déplacez le commentaire de la ligne qui fait référence au fichier itm_event.rules.

   Pour connaître les étapes détaillées, voir Mises à jour des fichiers de règles de la sonde EIF dans la documentation d'IBM Tivoli Monitoring.
3. Mettez à jour le schéma de base de données Netcool/OMNIbus ObjectServer en chargeant le fichier itm_apm_db_update.sql dans la base de données :

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user nom_utilisateur -password mot_de_passe
   -server nom_serveur > itm_apm_db_update.sql
   ```

   Exemple :

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS >
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U nom_utilisateur
   -P mot_de_passe -S nom_serveur
   ```

   Exemple :

   ```
   \temp\apm\itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U smadmin
   -P passw0rd -S NCOMS
   ```

   Les messages d'erreur suivants peuvent s'afficher lors de l'exécution des scripts (ces messages sont inoffensifs) :

- `Object exists` et `Attempt to insert duplicate row`, si les scripts ont été exécutés précédemment (par exemple, pour l'intégration à une version antérieure d'Cloud APM ou à Tivoli Monitoring).
- `ERROR=Object not found on line 4 of statement "-- A workspace table for the ITM event clear automation..."` sur ou près d'`itm_event_clear`.
- `ERROR=Object not found on line 1 of statement "delete from alerts.itm_problem_events;..."` sur ou près d'`itm_problem_events`.
- `ERROR=Object not found on line 1 of statement "drop table alerts.itm_problem_events;..."` sur ou près d'`itm_problem_events`.

4. Répétez l'étape 3 de sorte que le fichier soit chargé sur le serveur d'objets deux fois afin de garantir que toutes les dépendances soient correctement chargées.
5. Démarrez (ou redémarrez) Probe for Tivoli EIF.
6. Configurez le serveur Cloud APM pour acheminer les événements à Netcool/OMNIbus :
   a. Connectez vous à la console Cloud APM.
   b. Sélectionnez **Configuration du système** > **Configuration avancée**.
   c. Dans la catégorie Gestionnaire d'événements, définissez la zone **Cible(s) d'événement de fonction d'intégration d'événements** de sorte qu'elle inclut le nom d'hôte ou l'adresse IP de l'hôte sur lequel Netcool/OMNIbus est installé.
   d. Si nécessaire, modifiez le paramètre **Port de la fonction d'intégration d'événements** en fonction de votre environnement.
   e. Cliquez sur **Sauvegarder**.
7. Facultatif : lorsque vous créez ou éditez un seuil dans l'Editeur de seuils, définissez **Acheminer l'événement de fonction d'intégration d'événements** sur `Non` si vous ne souhaitez pas acheminer les événements au récepteur EIF. Pour plus d'informations, voir Acheminer l'événement de fonction d'intégration d'événements.

Résultats

Votre intégration Netcool/OMNIbus est maintenant terminée.

Si vos systèmes ObjectServer Probe for Tivoli EIF et Netcool/OMNIbus sont déjà intégrés à IBM Tivoli Monitoring, IBM SmartCloud Monitoring - Application Insight, IBM SmartCloud Application Performance Management ou Cloud APM, cette configuration active de nouvelles zones.

Que faire ensuite

Pour personnaliser le mappage des seuils aux événements transmis et remplacer ainsi le mappage par défaut entre les seuils et les événements transmis au serveur d'événements, cliquez sur **Personnalisation de l'attribut EIF** dans l'**Editeur de seuils**. Pour plus d'informations, voir Personnalisation d'un événement à transmettre à un récepteur EIF.

Intégration à Operations Analytics - Log Analysis

Si votre environnement inclut IBM Operations Analytics - Log Analysis, vous pouvez l'intégrer pour permettre les recherches dans les journaux d'application de la console Cloud APM.

Pourquoi et quand exécuter cette tâche

L'intégration à votre application Log Analysis installée implique de configurer le serveur Cloud APM avec l'adresse URL. Pour plus d'informations sur Log Analysis, voir IBM Operations Analytics - Developers Community.

Vous devez fournir l'URL de niveau supérieur pour votre installation de Log Analysis, par exemple :
`https://loganalysis.example.com:9987/Unity`

Procédure

1. Dans console Cloud APM, cliquez sur **Configuration du système** > **Configuration avancée**.
2. Sélectionnez la catégorie **Intégration de l'interface utilisateur**.
3. Dans la zone **URL d'analyse de journal**, entrez l'URL utilisée pour lancer votre application Log Analysis.

Résultats

L'application Log Analysis est intégrée et la fonction de recherche dans les journaux d'application à partir du Tableau de bord d'Application Performance est activée.

Que faire ensuite

Sélectionnez **Performance** > **Tableau de bord d'Application Performance**. Vous pouvez éventuellement sélectionner une application, puis utilisez la zone de recherche pour rechercher des fichiers journaux. Par défaut, les entrées sont recherchées sur la dernière heure, mais vous pouvez modifier cette plage de temps. Si vous sélectionnez une application, seuls les journaux sur les serveurs associés à cette application sont recherchés. Pour plus d'informations, voir «Recherche dans les fichiers journaux», à la page 1127.

Intégration à Operations Analytics - Predictive Insights

Lorsque vous intégrez IBM Cloud Application Performance Management à Operations Analytics - Predictive Insights, Operations Analytics - Predictive Insights analyse les données de mesure collectées par Cloud APM et génère des alarmes lorsqu'il identifie des anomalies dans les données.

Les anomalies sont affichées sous forme d'événements dans le tableau de bord de Cloud APM, comme décrit dans «Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights», à la page 1159. Vous pouvez ensuite effectuer une exploration en aval dans l'interface utilisateur d'Operations Analytics - Predictive Insights pour afficher plus de détails sur une anomalie.

Pour obtenir des instructions sur la configuration de l'intégration entre Operations Analytics - Predictive Insights et Cloud APM, voir Configuration de l'intégration avec IBM Performance Management dans le Knowledge Center d'IBM Operations Analytics - Predictive Insights.

Intégration à Alert Notification

Pour bénéficier d'une flexibilité plus grande que celle offerte par Cloud APM avec le transfert d'e-mail de base, vous pouvez effectuer une intégration au produit Alert Notification pour développer les capacités de Cloud APM en matière de notification des utilisateurs en cas de problèmes.

L'intégration à Alert Notification vous offre un contrôle granulaire sur les personnes qui reçoivent des notifications et sur la manière dont ces dernières leur parviennent. Par exemple, chaque utilisateur peut décider s'il souhaite recevoir des e-mails, des SMS ou des messages vocaux. Les notifications peuvent également être acheminées vers Slack. Des utilisateurs différents peuvent recevoir des types de notification différents en fonction du jour, du jour de la semaine, etc. Chaque utilisateur peut décider quels types d'alerte vous souhaitez recevoir. Par exemple, un administrateur de base de données peut souhaiter recevoir uniquement des alertes de base de données ayant un niveau de gravité avertissement ou supérieur.

Avant de commencer

Vous pouvez vous abonner à Alert Notification dans Marketplace ou IBM Cloud. Une fois abonné, vous recevrez un e-mail indiquant que votre service est prêt.

Remarque : Vous pouvez démarrer Alert Notification en vous connectant à votre compte d'abonnement sur IBM Marketplace et accéder à Produits et services.

Pourquoi et quand exécuter cette tâche

Dans le cadre de l'intégration à Alert Notification, vous devez configurer Cloud APM pour l'envoi d'événements à Alert Notification. Ensuite, vous pouvez créer des règles de notification afin de déterminer les alertes pour lesquelles vous souhaitez recevoir des notifications.

Vous pouvez ajouter l'application surveillée aux groupes de ressources. Pour chaque groupe de ressources sauvegardé, vous pouvez configurer une ou plusieurs adresses électroniques. Lorsque les performances d'un système géré dans un groupe dépasse un seuil, une notification par courrier électronique est envoyée aux adresses configurées pour le groupe.

Alert Notification envoie une notification par courrier électronique pour tous les événements ouverts sur les systèmes gérés affectés au groupe.

Procédure

Exécutez une fois les étapes 1 à 2 pour le déploiement de Cloud APM.

1. Dans l'interface utilisateur Alert Notification, obtenez les informations suivantes que vous utiliserez pour configurer Cloud APM pour l'intégration à Alert Notification :

   Noeud final d'API de notification d'alerte
   URL associée à l'API Alert Notification utilisée pour traiter les notifications d'alerte.

   Pour obtenir l'URL, ouvrez l'interface utilisateur d'Alert Notification et cliquez sur **Manage API Keys** et sur l'icône d'information. Copiez l'URL d'API affichée et collez-la dans cette zone.

   Clé d'API de notification d'alerte
   Clé créée dans l'interface utilisateur Alert Notification. Cette clé d'API est associée au mot de passe d'API entré avec ce paramètre de configuration.

   Pour obtenir la clé de l'API Alert Notification, voir Gestion des clés d'API.

   Mot de passe de l'API de notification d'alerte
   Mot de passe associé à la clé entrée avec le paramètre de configuration **`Alert Notification API Key`**.

   Pour obtenir le mot de passe de l'API Alert Notification, voir Gestion des clés d'API.

2. Dans APM Console, suivez la procédure ci-dessous pour configurer Cloud APM pour l'intégration à Alert Notification :
   a. Cliquez sur **Configuration du système** > **Configuration avancée** et sélectionnez **Gestionnaire d'événements**.
   b. Dans la liste **Paramètres** d'Event Manager, renseignez les zones Alert Notification suivantes :

      Noeud final d'API de notification d'alerte
      Dans cette zone, ajoutez l'URL d'API que vous avez obtenue à l'étape 1.

      Clé d'API de notification d'alerte

      Dans cette zone, ajoutez la clé d'API Alert Notification que vous avez obtenue à l'étape 1.

      Mot de passe de l'API de notification d'alerte
      Dans cette zone, ajoutez le mot de passe d'API Alert Notification que vous avez obtenu à l'étape 1.

      Notification d'alerte pour ITMv6
      Définissez cette valeur sur True pour activer la notification d'alerte pour les événements ITMv6. La valeur par défaut est False.

Exécutez les étapes 3 et 4 pour le groupe de ressources pour lequel vous souhaitez acheminer des alertes en fonction du groupe de ressources.

3. Si vous souhaitez acheminer les notifications en fonction des groupes de ressources, suivez les sous-étapes ci-dessous :
   a. Dans la console Cloud APM, cliquez sur **Configuration système** > **Gestionnaire de groupes de ressources**.
   b. Sélectionnez un groupe de ressources, puis cliquez sur **Editer** pour ouvrir l'Editeur de groupe de ressources.

      Important : Vous devez sauvegarder un groupe de ressources nouveau ou modifié avant d'ouvrir Alert Notification. Une fois la sauvegarde effectuée, l'éditeur de groupe de ressources se ferme et vous devez le rouvrir pour pouvoir continuer à l'utiliser.

      Si vous n'effectuez pas la sauvegarde, après avoir configuré des notifications par courrier électronique à l'étape 4 et être revenu à l'éditeur de groupe de ressources, vous risquez de recevoir un message d'erreur vous informant que la mise à jour synchrone n'est pas autorisée.
4. Pour configurer la notification par courrier électronique, procédez comme suit :
   a. Dans l'éditeur de groupe de ressources d'APM Console, cliquez sur l'URL **Configurer la notification par courrier électronique** pour ouvrir l'application IBM Alert Notification dans un nouvel onglet ou une nouvelle fenêtre. Cette action crée automatiquement une règle basée sur le groupe de ressources que vous avez sélectionné à l'étape 3.

      Avertissement : Si votre navigateur n'autorise pas les fenêtres en incrustation, la fenêtre Alert Notification ne peut pas s'ouvrir. Vous devez configurer le navigateur de manière à autoriser la fenêtre Alert Notification à s'ouvrir pour pouvoir configurer la notification par courrier électronique d'un groupe de ressources.
   b. Dans Alert Notification, configurez des utilisateurs et des groupes et associez leurs adresses électroniques à des groupes de ressources pour que ceux-ci reçoivent des notifications d'événements par courrier électronique.

      Vous pouvez configurer vos propres règles et notifications Alert Notification pour le type d'alertes que vous souhaitez recevoir. Par exemple, un administrateur Linux peut souhaiter recevoir des e-mails, des messages SMS ou des messages vocaux pour l'ensemble des systèmes Linux. Ensuite, il peut décider de désactiver les alertes de forte gravité qui sont critiques. Une règle leur permet de filtrer tous les événements qui sont générés par l'agent de système d'exploitation Linux. Pour des informations sur l'utilisation de l'éditeur de notifications dans l'application Alert Notification, voir Création de règles de notification.

Que faire ensuite

Pour plus d'informations sur Alert Notification, voir la Documentation d'IBM Alert Notification.

Intégration à IBM Cloud

Vous pouvez afficher les informations de surveillance relatives à vos applications dans l'environnement IBM Cloud à l'aide des collecteurs de données sélectionnés.

Lorsqu'il est configuré pour collecter les données d'une application IBM Cloud, un collecteur de données permet l'intégration des fonctionnalités de surveillance à IBM Cloud. Les collecteurs de données transfèrent les données de surveillance et de diagnostic des ressources relatives à vos applications IBM Cloud au serveur Cloud APM. Le serveur Cloud APM reçoit et traite les informations de surveillance qui sont collectées par les collecteurs de données. Les types d'applications IBM Cloud suivants peuvent être surveillés :

- Applications Liberty

- Applications Node.js
- Applications Python
- Applications Ruby

Après configuré correctement un collecteur de données, vous pouvez afficher les données de surveillance sur la console Cloud APM. Pour obtenir des instructions de configuration, voir «Configuration des collecteurs de données», à la page 232.

Surveillance d'IBM Cloud Private

Vous pouvez utiliserIBM Cloud Application Performance Management, Private pour surveiller votre environnement IBM Cloud Private afin de gérer les charges de travail traditionnelles et basées sur les conteneurs depuis la console Cloud APM.

Surveillance de vos conteneurs IBM Cloud Private

Utilisez IBM Cloud Application Performance Management, Private pour surveiller les conteneurs IBM Cloud Private dans lesquels vos charges de travail s'exécutent.

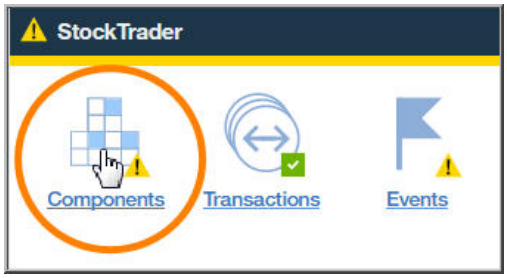
La configuration comprend certaines étapes de base :

Installation de l'agent Linux OS sur les noeuds Cloud Private
Vous installez l'agent Linux OS Cloud APM à la fois sur les noeuds d'agents et les noeuds principaux Cloud Private. Il est recommandé d'inclure l'agent Linux OS installé pour chaque machine virtuelle créée pour IBM Cloud Private. Pour plus d'informations, voir «Installation des agents sur les systèmes Linux», à la page 170.

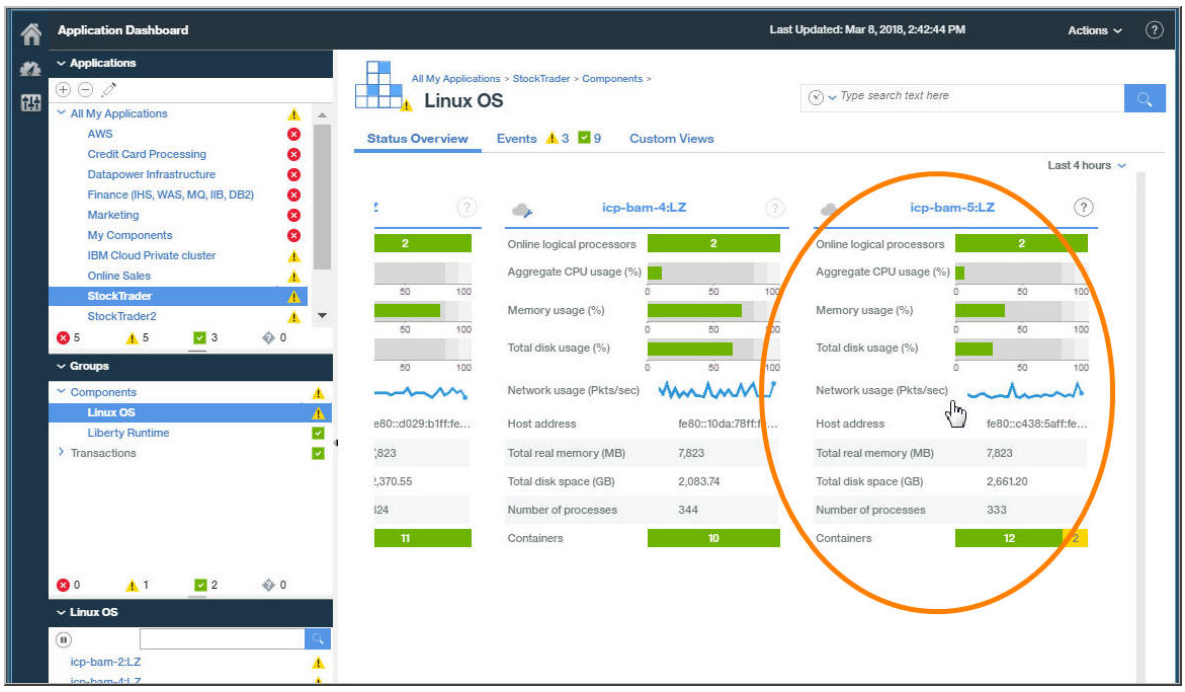
Création d'une application pour regrouper les ressources de système d'exploitation
Pour gérer les noeuds qui composent le conteneur Cloud Private, créez une application pour les regrouper. Lancez la console Cloud APM et créez une application avec les ressources gérées par Linux OS que vous avez installées dans votre environnement Cloud Private. Pour plus d'informations, voir «Gestion des applications», à la page 1145.

Démarrage de la surveillance de votre conteneur Cloud Private
Maintenant, vous êtes prêt à utiliser la console Cloud APM pour surveiller le conteneur Linux OS. Examinez rapidement les tableaux de bord de l'application que vous avez créée. Les exemples donnés dans ces écrans présentent l'application Stock Trader qui a été créée pour surveiller le conteneur Cloud APM.

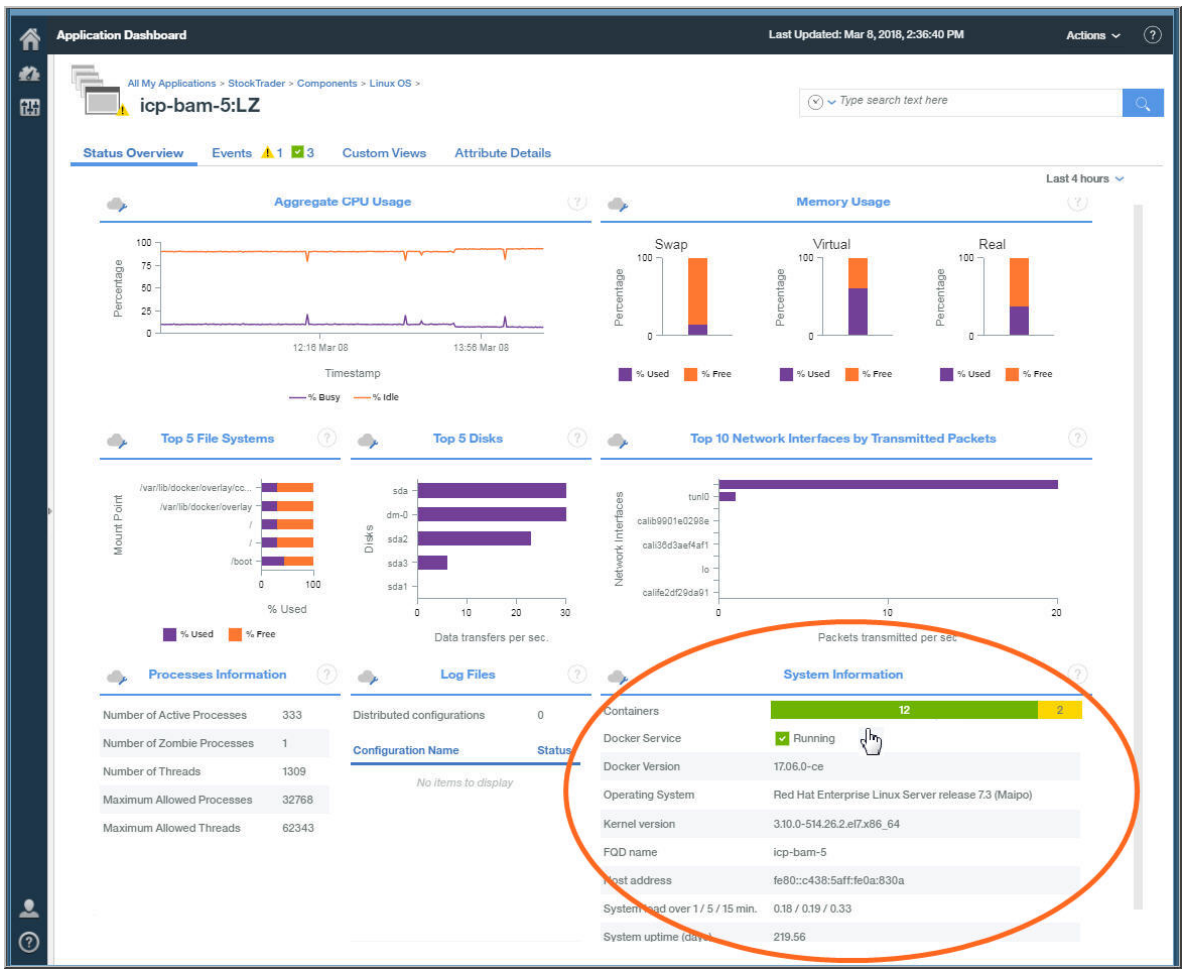
Après avoir démarré la console Cloud APM, cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**. Recherchez la zone de statut récapitulative de StockTrader et sélectionnez **Composants** pour obtenir une présentation des statuts de toutes les ressources gérées.



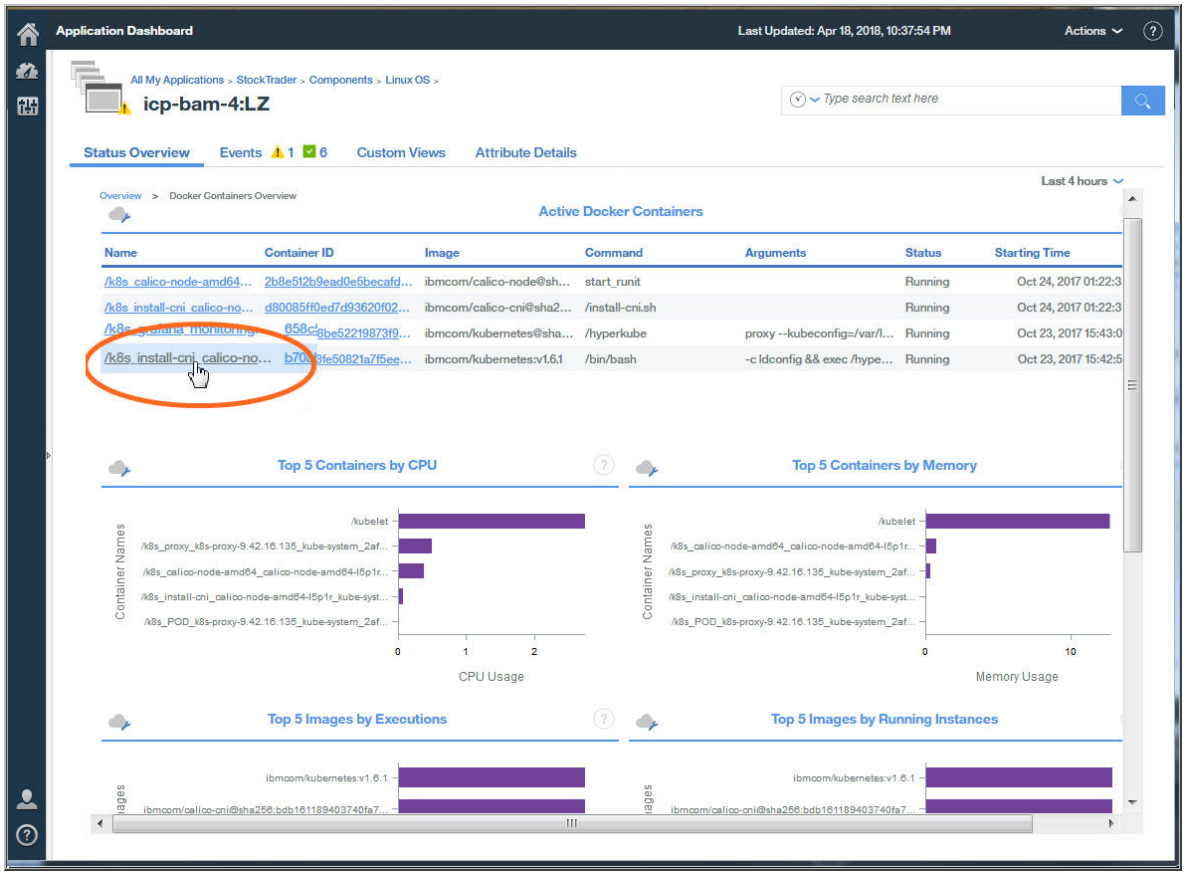
La présentation des statuts s'affiche avec un widget de groupe pour chaque ressource gérée dans l'application Stock Trader. Vous pouvez déplacer la souris sur l'un de ces widgets pour visualiser la valeur exacte, comme le pourcentage d'utilisation d'UC agrégée. Au niveau de groupe du navigateur, le statut apparaît pour chaque ressource gérée dans l'application.



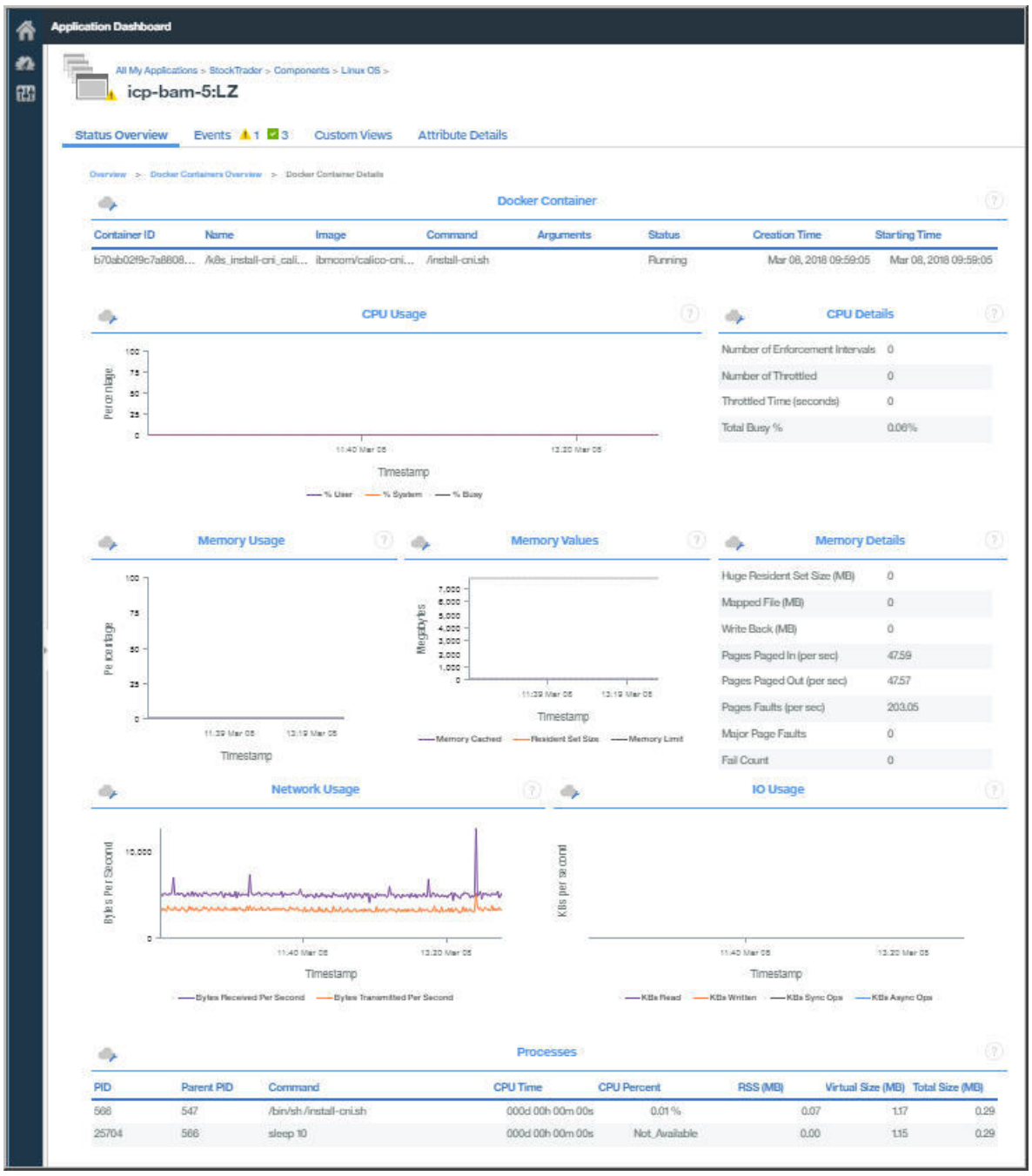
Cliquez dans le widget de groupe Linux OS pour ouvrir le tableau de bord pour le noeud. Le tableau de bord **Présentation** présente les statistiques Linux OS les plus intéressantes. Par exemple, le widget de groupe Informations système affiche le statut de tous les conteneurs, y compris la charge système et le temps d'activité.



Cliquez sur la jauge Conteneurs ou sur le widget Service Docker pour ouvrir la vue **Présentation des conteneurs Docker**. La table répertorie tous les conteneurs Docker actifs et affiche ceux qui consomment le plus d'UC et de mémoire, ainsi que les images de ceux pour lesquels les exécutions et les instances actives sont les plus nombreuses.



Cliquez sur une ligne de la table Conteneurs Docker actifs pour afficher plus de détails sur le conteneur. Le tableau de bord **Détails des conteneurs Docker** affiche des informations sur le conteneur Docker, les statistiques sur les performances au cours des quatre dernières heures que vous pouvez étendre à une journée entière ou comparer à celles d'un autre jour, ainsi que d'autres informations telles que les processus en cours d'exécution et la quantité d'UC qu'ils consomment.



Vous pouvez également utiliser des seuils prédéfinis pour surveiller la consommation des ressources Linux OS par le conteneur Cloud Private. Créez des seuils afin de détecter les problèmes de manière précoce. Pour plus d'informations sur l'ajout de seuils, voir «Tutoriel : Définition d'un seuil», à la page 998.

Surveillance de vos applications IBM Cloud Private

Utilisez IBM Cloud Application Performance Management, Private pour surveiller vos applications basées sur Liberty IBM Cloud Private.

La configuration comprend certaines étapes de base :

Configuration du collecteur de données Liberty pour la connexion au serveur Cloud APM

Lorsque vous configurez un pipeline Microservice Builder et que vous insérez une application Liberty dans Cloud Private, le collecteur de données Liberty est installé automatiquement. Ce collecteur de données présente initialement l'état Désactivé et s'active une fois les informations de serveur Cloud APM découvertes. Vous utilisez les secrets Kubernetes pour fournir les informations de serveur.

Vous pouvez également déployer le collecteur de données Liberty dans Cloud Private sans utiliser Microservice Builder.

Pour plus d'informations, voir Configuring data collection for Java-based microservices or Liberty applications sur le APM Developer Center.

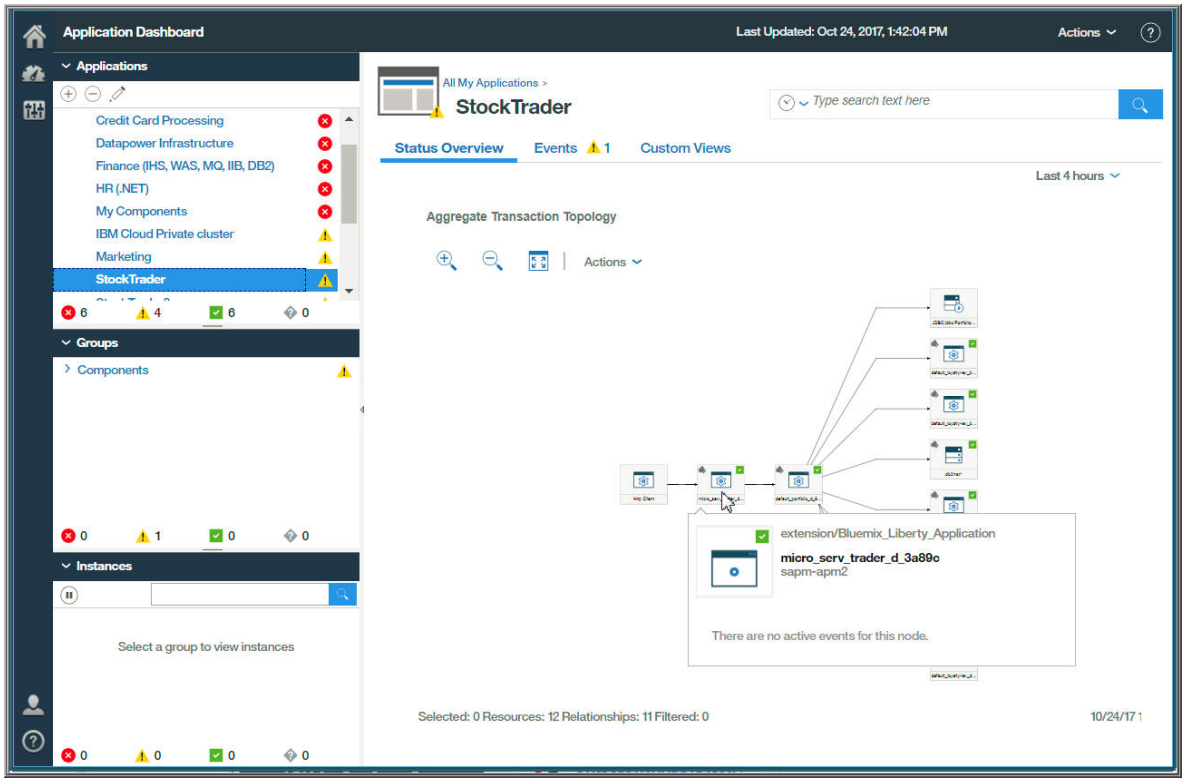
Ajout d'une application pour la gestion de vos applications Cloud Private

Pour gérer vos applications basées sur Liberty, regroupez-les en ajoutant une application dans le Tableau de bord d'Application Performance. Lancez la console Cloud APM et créez une application avec les ressources gérées Liberty que vous avez configurées dans votre environnement Cloud Private. Pour plus d'informations, voir «Gestion des applications», à la page 1145.

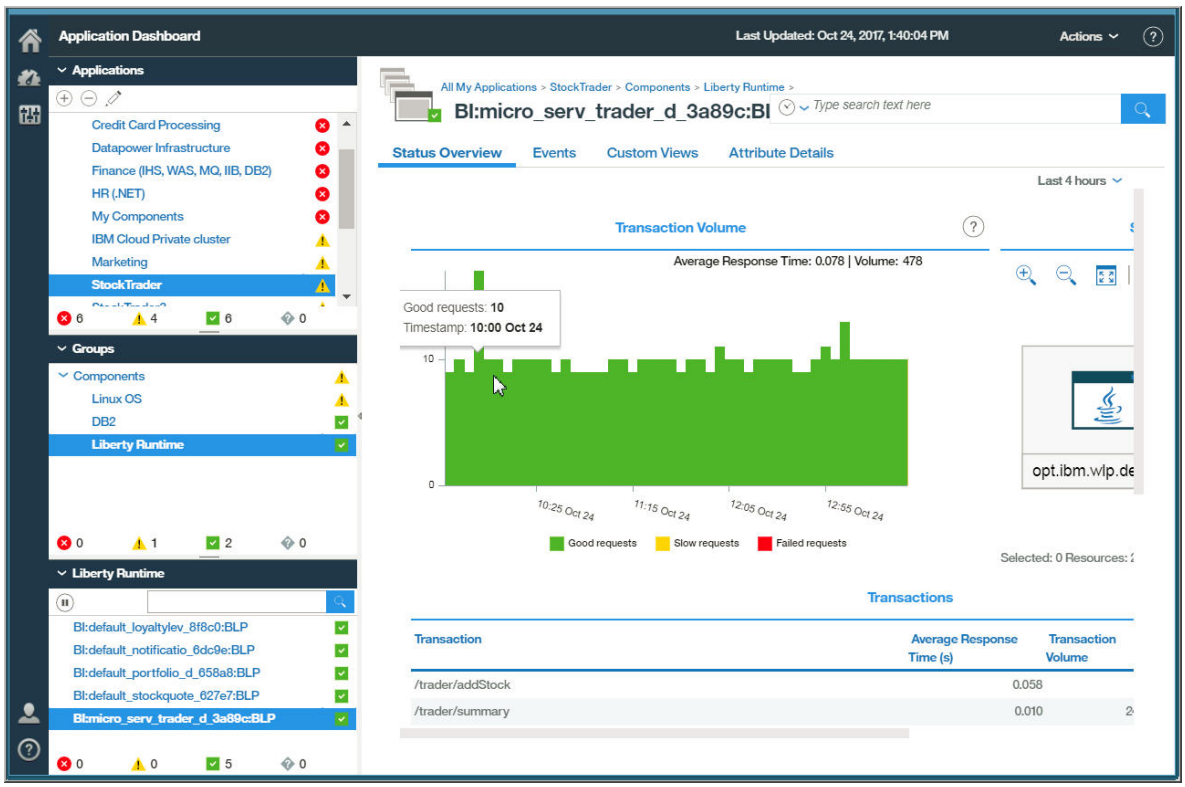
Démarrage de la surveillance de vos applications Cloud Private

A présent, vous êtes prêt à utiliser la console Cloud APM pour surveiller vos applications Microservice basées sur Liberty. Jetez un coup d'oeil aux tableaux de bord de l'application que vous avez créée afin de déterminer rapidement l'origine des problèmes liés aux microservices. Les exemples donnés dans ces écrans présentent l'application Stock Trader qui a été créée pour surveiller les applications Cloud Private basées sur Liberty.

Le tableau de bord au niveau de l'application présente la vue Agréger une topologie de transaction. Survolez un noeud avec le pointeur de la souris pour afficher des informations supplémentaires.



Cliquez avec le bouton droit de la souris sur un noeud et sélectionnez **Accéder à la Page Récapitulatif des transactions**.



Des détails sur les transactions sont affichés pour l'instance Liberty Runtime dans le tableau de bord. Le graphique à barres Volume de transactions indique le volume et le temps de réponse moyen. Dans la table Transactions, vous pouvez cliquer sur une transaction pour l'examiner en détail.

Vous pouvez exploiter les seuils prédéfinis pour surveiller vos applications basées sur Liberty Cloud Private. Ajoutez des seuils supplémentaires pour détecter les problèmes de manière précoce, tels qu'un taux d'échecs des transactions élevé sur Liberty. Pour plus d'informations sur l'ajout de seuils, voir «Tutoriel : Définition d'un seuil», à la page 998.

Intégration à Tivoli Common Reporting

Intégrez Tivoli Common Reporting à Cloud APM pour générer des rapports sur les données qui sont collectées par l'Agent de surveillance des temps de réponse, l'Agent Synthetic Playback et l'Agent WebSphere Applications. Les rapports sont disponibles uniquement pour l'exécution de Tivoli Common Reporting sur des systèmes Linux et AIX.

Intégration de Tivoli Common Reporting à Cloud APM

Si vous prévoyez d'intégrer Tivoli Common Reporting à Cloud APM, utilisez Tivoli Common Reporting version 3.1.2.1 ou 3.1.3 sur les systèmes Linux ou AIX.

Tivoli Common Reporting version 3.1.2.0 est inclus dans Jazz for Service Management version 1.1.2.0. Jazz for Service Management version 1.1.2.0 est un composant de Tivoli Monitoring version 6.3.0.7, qui est fourni avec Cloud APM version 8.1.4. Vous devez installer le groupe de correctifs 1 de Jazz for Service Management version 1.1.2, ce qui met à niveau Jazz for Service Management vers la version 1.1.2.1 et Tivoli Common Reporting vers la version 3.1.2.1. Pour obtenir les numéros de référence eAssembly et eImage applicables, voir «Numéros de référence», à la page 118.

Tivoli Common Reporting version 3.1.3 est inclus dans Jazz for Service Management version 1.1.3. Voir la dernière mise à jour du Knowledge Center de Jazz for Service Management version 1.1.3.0.

Pour intégrer Tivoli Common Reporting, vous devez effectuer les tâches suivantes :

1. Téléchargez et installez Tivoli Common Reporting.
2. Vérifiez que le serveur Tivoli Common Reporting est connecté à la machine Db2 de Cloud APM. Sinon, configurez une connexion ODBC entre le serveur Tivoli Common Reporting et la machine Db2 de Cloud APM.
3. Configurez l'image d'installation des rapports afin de créer le package de rapports.
4. Installez le module de rapports sur le serveur Tivoli Common Reporting.
5. Activez la connexion unique entre Cloud APM et Tivoli Common Reporting.

Pour obtenir la liste des rapports disponibles pour chaque agent, voir «Rapports», à la page 1172.

Téléchargement et installation de Tivoli Common Reporting

Avant d'intégrer Tivoli Common Reporting à Cloud APM, vous devez télécharger et installer Tivoli Common Reporting.

Tivoli Common Reporting est un composant de Jazz for Service Management. Il s'agit d'un prérequis pour les rapports de l'Agent de surveillance des temps de réponse, l'Agent Synthetic Playback et l'Agent WebSphere Applications. Les rapports de Cloud APM ne sont pris en charge que sur les systèmes Tivoli Common Reporting Linux.

Tivoli Common Reporting fait partie de IBM Tivoli Monitoring et est regroupé avec les offres Cloud APM. L'image à télécharger est disponible depuis le site Web de IBM Passport Advantage. Pour plus d'informations sur le téléchargement, voir Chapitre 6, «Instructions de téléchargement», à la page 115. Pour plus d'informations surTivoli Common Reporting, voir la dernière mise à jour de Knowledge Center de Jazz for Service Management Version 1.1.3.0.

Configuration d'une connexion ODBC

Avant d'installer des rapports Cloud APM, vous devez configurer une connexion ODBC entre le serveur Tivoli Common Reporting et le système Cloud APM Db2. Cette configuration permet à Tivoli Common Reporting d'extraire les données nécessaires de la base de données Cloud APM Db2 à l'aide d'un client Db2 local.

Procédure

1. Sur le serveur Tivoli Common Reporting, connectez-vous à la base de données Cloud APM Db2 à l'aide du client Db2 et cataloguez un noeud. Exécutez la commande suivante :

   ```
   su - utilisateur_instance_bd_locale
   db2 catalog tcpip node nom_noeud_db2_apm remote adresse_ip_db2_apm server port_instance_db2_apm
   ```

   Exemple :

   ```
   su - dbinst1
   db2 catalog tcpip node DB2_SRVR remote 123.456.789.123 server 50000
   ```

   Le *nom_noeud_db2_apm* doit comporter plus de 8 caractères.
2. Sur le serveur Tivoli Common Reporting, connectez-vous à l'instance Db2 locale et cataloguez les bases de données WAREHOUS et DATAMART de Db2 Cloud APM :

   Pour créer une connexion afin de générer des rapports pour Agent WebSphere Applications, exécutez la commande suivante :

   ```
   su - utilisateur_instance_bd_locale db2 catalog db WAREHOUS as WAREHOUS at node nom_noeud_db2_apm
   ```

   Exemple :

   ```
   su - dbinst1
   db2 catalog db WAREHOUS as WAREHOUS at node DB2_SRVR
   ```

Pour créer une connexion afin de générer des rapports pour l'Agent Synthetic Playback ou l'Agent de surveillance des temps de réponse, vous devez cataloguer la base de données Db2 DATAMART. Exécutez la commande suivante :

```
su - db2inst1
db2 catalog db DATAMART as DATAMART at node nom_noeud_db2_apm
```

Exemple :

```
su - dbinst1
db2 catalog db DATAMART as DATAMART at node DB2_SRVR
```

Si vous utilisez des noms de base de données personnalisés à la place des noms de base de données WAREHOUSE et DATAMART par défaut, cataloguez WAREHOUS et DATAMART comme indiqué ci-dessous :

```
su - utilisateur_instance_bd_locale
db2 catalog db CUSTOM_WAREHOUS_DBNAME as WAREHOUS at node nom_noeud_db2_apm
db2 catalog db CUSTOM_DATAMART_DBNAME as DATAMART at node nom_noeud_db2_apm
```

Résultats

Une connexion ODBC est maintenant configurée entre le serveur Tivoli Common Reporting et le client Db2.

Que faire ensuite

Configurez l'image d'installation des rapports. Pour plus d'informations, voir «Configuration de l'image d'installation des rapports».

Configuration de l'image d'installation des rapports

Avant d'installer les rapports Cloud APM, vous devez configurer l'image d'installation des rapports pour établir une connexion avec le serveur Cloud APM. Lorsque vous réalisez la configuration, un module de rapports est créé pour l'installation.

Avant de commencer

1. Veillez à configurer la connexion ODBC entre le serveur Tivoli Common Reporting et la machine Db2 de Cloud APM. Pour plus d'informations, voir «Configuration d'une connexion ODBC», à la page 918.
2. Téléchargez l'image des rapports sur le serveur Cloud APM. Pour les détails, voir Chapitre 6, «Instructions de téléchargement», à la page 115. Les images d'installation des rapports suivantes sont disponibles selon votre offre :
   - `apm_advanced_reports_8.1.4.0.zip`
   - `apm_base_reports_8.1.4.0.zip`

Procédure

1. Exécutez le script `configure_reports_images.sh` avec des privilèges de superutilisateur pour configurer l'image d'installation des rapports :

   ```
   /opt/ibm/ccm/configure_reports_images.sh
   ```

   Où `/opt/ibm/` est le dossier d'installation par défaut du serveur Cloud APM. Si le dossier d'installation du serveur Cloud APM est différent, remplacez `/opt/ibm/` par l'emplacement du dossier d'installation.
2. Entrez 1 pour confirmer la configuration de l'image d'installation des rapports.
3. Entrez le chemin du répertoire dans lequel vous avez téléchargé l'image d'installation des rapports.
4. Entrez le mot de passe de l'utilisateur smadmin de Cloud APM.

Important : Il s'agit du mot de passe de l'utilisateur smadmin Cloud APM interne. Le mot de passe smadmin est identique au mot de passe de l'utilisateur apmadmin que vous avez indiqué lors de l'installation. La valeur par défaut est `apmpass`. Si vous n'arrivez pas à vous rappeler le mot de passe smadmin, vous pouvez le modifier en vous servant du script décrit dans la rubrique suivante : «Utilisateurs et mots de passe par défaut», à la page 1075.
Une fois que vous avez entré le mot de passe approprié, le script de configuration configure l'image d'installation des rapports et copie le module de rapports dans un autre répertoire.

5. Entrez le chemin au niveau duquel vous voulez stocker le module de rapports ou acceptez la valeur par défaut **`/opt/ibm/ccm/depot`**.
6. Entrez le nom d'hôte complet du serveur Cloud APM avec lequel le serveur Tivoli Common Reporting communique pour extraire les données des rapports. Pour plus d'informations sur Tivoli Common Reporting, voir «Téléchargement et installation de Tivoli Common Reporting», à la page 918.

Résultats

Un message s'affiche pour indiquer le répertoire où se trouve le module d'installation des rapports.

Le module d'installation des rapports se trouve dans le répertoire que vous avez indiqué à l'étape 5. Il porte le même nom que l'image d'installation des rapports que vous avez téléchargée. Par exemple, si vous avez téléchargé le fichier `apm_advanced_reports_8.1.4.0.zip` et que vous avez correctement effectué la configuration, le module d'installation des rapports `apm_advanced_reports_8.1.4.0.zip` se trouve dans le répertoire que vous avez indiqué à l'étape 5.

Que faire ensuite

Installez les modules de rapports. Pour plus de détails, voir «Installation des rapports».

Installation des rapports

Installez le module de rapports sur le serveur Tivoli Common Reporting.

Avant de commencer

Avant d'installer des rapports, vous devez effectuer les tâches suivantes :

- Configurez l'image d'installation des rapports. Si vous avez configuré l'image d'installation des rapports, l'un des modules d'installation des rapports suivants apparaît dans le répertoire que vous avez indiqué lors de la configuration. Le dossier par défaut du module d'installation par défaut est `/opt/ibm/ccm/depot`.
  - `apm_advanced_reports_8.1.4.0.zip`
  - `apm_base_reports_8.1.4.0.zip`

  Pour plus d'informations, voir «Configuration de l'image d'installation des rapports», à la page 919.
- Vérifiez que la connectivité du réseau existe entre le serveur Tivoli Common Reporting et le serveur Cloud APM. Le script `install_reports.sh` utilise le port 8090 pour envoyer les requêtes HTTP au serveur Cloud APM.

Procédure

1. Copiez le module d'installation des rapports du serveur Cloud APM sur le serveur Tivoli Common Reporting et extrayez-le.
2. Sur le serveur Tivoli Common Reporting, exécutez le script d'installation avec les droits utilisateur root :

   ```
   ./installReports.sh
   ```

Remarque : AIX Si vous voulez installer des packages de rapports sur un système AIX avec l'interpréteur de commandes Korn défini comme valeur par défaut, vous devez vous assurer que l'interpréteur de commandes Bash est disponible. Vous devez également éditer le script `./installReports.sh` pour changer la ligne

```
#!/bin/sh
```

par

```
#!/bin/bash
```

3. Sélectionnez les packages à installer à partir des packages de rapports suivants en entrant les numéros correspondants :
   - Rapports de l'Agent de surveillance des temps de réponse (indisponible dans IBM Cloud Application Performance Management, Base Private)
   - Rapports de l'Monitoring Agent for WebSphere Applications
   - Rapports de l'Monitoring Agent for Synthetic Playback (indisponible dans IBM Cloud Application Performance Management, Base Private)
4. Saisissez le chemin d'installation de Jazz for Service Management.
5. Saisissez le nom d'utilisateur et le mot de passe pour un utilisateurJazz for Service Management avec des droits d'administrateur.
6. Entrez le mot de passe de l'administrateur Cloud APM.

   Important : Il s'agit du mot de passe de l'utilisateur smadmin Cloud APM interne. Le mot de passe smadmin est identique au mot de passe de l'utilisateur apmadmin que vous avez indiqué lors de l'installation. La valeur par défaut est `apmpass`. Si vous n'arrivez pas à vous rappeler le mot de passe smadmin, vous pouvez le modifier en vous servant du script décrit dans la rubrique suivante : «Utilisateurs et mots de passe par défaut», à la page 1075.
7. Saisissez le nom d'hôte complet de Tivoli Common Reporting. Pour plus d'informations sur Tivoli Common Reporting, voir «Téléchargement et installation de Tivoli Common Reporting», à la page 918.
8. Vérifiez les paramètres Cognos Application Firewall et Cross Site Scripting (XSS) dans IBM Cognos et Cloud APM pour permettre l'accès aux rapports depuis le Tableau de bord d'Application Performance.
   a. Accédez à l'emplacement d'installation de Tivoli Common Reporting et exécutez Cognos Configuration. L'emplacement par défaut est le suivant :
      - Windows `C:\Program Files\IBM\JazzSM\reporting\cognos\bin64\tcr_cogconfig.bat`
      - Linux `/opt/IBM/JazzSM/reporting/cognos/bin64/tcr_cogconfig.sh`
   b. Dans le tableau Component Properties, vérifiez que **Enable CAF validation?** et **Is third party XSS checking enabled?** sont définis sur `True`. Pour plus d'informations, voir Configuration des composants IBM Cognos pour qu'ils utilisent IBM Cognos Application Firewall.
   c. Redémarrez le serveur Tivoli Common Reporting. Pour plus d'informations, voir Redémarrage des serveurs d'applications Jazz for Service Management.
   d. Dans la console console Cloud APM, cliquez sur **Configuration avancée** > **Intégration d'UI** > **Paramètres** et définissez **Cognos Reporting Requires XSS Validation** sur `True`.

Résultats

Les modules de rapports sont correctement installés. L'adresse URL de Tivoli Common Reporting est ajoutée à la zone **Cognos Reporting URL** dans **Configuration avancée** > **Intégration d'UI** > **Paramètres** de la console Performance Management. Le format d'URL de génération de rapports Cognos est le suivant : `https://`*`nomhôte_serveur_générationrapports`*`:`*`port`*`/tarf/servlet/dispatch/secured`.

Pour Tivoli Common Reporting 3.1.1 et version ultérieure, le format d'URL de génération de rapports Cognos est le suivant : `https://nomhôte_serveur_générationrapports:port/tarf/servlet/reporting/secured`.

Si vous utilisez Tivoli Common Reporting 3.1.1 ou version ultérieure, vous devez utiliser la console Cloud APM pour définir manuellement la zone **URL de Cognos Reporting** dans la section **Configuration avancée** > **UI Configuration** > **Paramètres**.

Important : Si le script d'installation ne s'exécute pas correctement, examinez les messages d'erreur dans le dernier fichier journal disponible dans le répertoire `/tmp/apm_reports_installer`.

Que faire ensuite

Vous êtes maintenant prêt à afficher les rapports dans le Tableau de bord des applications. Pour plus d'informations, voir «Rapports», à la page 1172.

Configuration de la connexion unique avec Tivoli Common Reporting

Désactivez OIDC, puis configurez Tivoli Common Reporting et IBM Cloud Application Performance Management pour activer la connexion unique (SSO) et éviter les requêtes de connexion répétées.

Pour activer la connexion unique entre Tivoli Common Reporting et Cloud APM, vous devez effectuer les tâches suivantes :

1. Désactivez l'authentification OpenID Connect pour l'interface utilisateur de Cloud APM.
2. Activez la connexion unique entre Cloud APM et Tivoli Common Reporting.
3. Vérifiez que l'hôte **URL Cognos Reporting** est le nom d'hôte qualifié complet du serveur Tivoli Common Reporting sous **Configuration avancée** > **Intégration de l'interface utilisateur**. Pour plus d'informations, voir «Installation des rapports», à la page 920.

Désactivation de l'authentification OpenID Connect pour la console Cloud APM

Vous devez désactiver l'authentification OpenID Connect pour la console Cloud APM avant d'activer la connexion unique (SSO) entre Cloud APM et un autre produit IBM nécessitant LTPA pour SSO.

Bien que OIDC ne soit plus utilisé pour l'authentification d'UI après la mise en place de cette procédure, les API RESTful continuent de se fier à OIDC. Les API RESTful n'interfèrent pas avec SSO (voir «Exploration des API», à la page 1115).

Procédure

Procédez comme suit pour désactiver l'authentification OIDC pour la console Cloud APM.

1. Arrêtez tous les serveurs avec la commande `apm stop_all`. Pour plus d'informations, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.
2. Si LDAP est déjà configuré pour Cloud APM, vous devez temporairement modifier le fichier `commonRegistry.xml`, situé dans *rép_install*`/wlp/usr/shared/config/`, afin d'inclure `basicRegistry.xml` à la place de `ldapRegistry.xml` :
   a. Placez en commentaire la ligne qui fait référence au fichier de registre LDAP, de la manière suivante :
      ```
      <!--include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/-->
      ```
   b. Supprimez les balises de commentaire de la ligne qui fait référence au fichier de registre de base, de la manière suivante :
      ```
      <include optional="false" location="${shared.config.dir}/basicRegistry.xml"/>
      ```
3. Modifiez la valeur de l'attribut oauthRealm dans le fichier *rép_install*`/wlp/usr/shared/config/oauthVariables-onprem.xml` de sorte qu'elle corresponde à la valeur de l'attribut realm dans le fichier `basicRegistry.xml`.

4. Pour éditer le fichier *rép_install*/wlp/usr/servers/apmui/server-oauth2-tai.xml afin de supprimer temporairement la propriété **systemUser**, procédez comme suit :
   a. Effectuez une copie de sauvegarde du fichier *rép_install*/wlp/usr/servers/apmui/server-oauth2-tai.xml.
   b. Ouvrez le fichier *rép_install*/wlp/usr/servers/apmui/server-oauth2-tai.xml et recherchez la ligne qui commence par <properties. Supprimez la propriété **systemUser**.
5. Editez le fichier *rép_install*/wlp/usr/servers/apmui/server.xml et mettez en commentaire cette ligne comme suit :
   ```
   <!--include optional="true" location="server-relying-party.xml"/-->
   ```
6. Editez le fichier *rép_install*/wlp/usr/servers/apmui/server-itportal.xml de façon à modifier la ligne suivante :
   ```
   <application type="eba" id="Blaze" name="Blaze"
      location="${server.config.dir}/apps/com.ibm.tivoli.blaze_2.3.0.7.eba">
   ```
   Modifiez la ligne comme suit :
   ```
   <application type="eba" id="Blaze" name="Blaze"
        location="${server.config.dir}/apps/com.ibm.tivoli.blaze_2.3.0.7.ltpasso.eba">
   ```
7. Editez le fichier *rép_install*/wlp/usr/servers/uviews/server.xml et mettez en commentaire cette ligne comme suit :
   ```
   <!--include optional="true" location="server-relying-party.xml"/-->
   ```
   Vous devez utiliser le format exact illustré ici pour mettre en commentaire l'instruction include pour le fichier server-relying-party.xml.
8. Exécutez la commande suivante à l'aide du mot de passe correct de l'utilisateur **apmadmin** :
   rép_install/ccm/configureConsole_ltpasso.sh **apmadmin** *mot_de_passe*
   Le *mot_de_passe* par défaut est **apmpass**.
9. Si vous avez désactivé LDAP à l'étape 2, à la page 922, réactivez le registre LDAP dans le fichier commonRegistry.xml :
   a. Placez en commentaire la ligne qui fait référence au registre de base, de la manière suivante :
      ```
      <!--include optional="false" location="${shared.config.dir}/basicRegistry.xml"/-->
      ```
   b. Supprimez les balises de commentaire de la ligne qui fait référence au fichier de registre LDAP, de la manière suivante :
      ```
      <include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/>
      ```
10. Si vous avez modifié la valeur de l'attribut oauthRealm à l'étape 3, à la page 922, mettez-la à jour pour qu'elle corresponde à la valeur de l'attribut realm dans le fichier ldapRegistry.xml.
11. Si vous avez supprimé la propriété **systemUser** à l'étape 4, remplacez le fichier *rép_install*/wlp/usr/servers/apmui/server-oauth2-tai.xml actuel par le fichier de sauvegarde que vous avez créé à l'étape 4a.
12. Démarrez tous les serveurs avec la commande apm restart_all. Pour plus d'informations, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.

Résultats

L'authentification OpenID Connect pour la console Cloud APM est maintenant désactivée.

Activation de la connexion unique entre Cloud APM et Tivoli Common Reporting

Configurez Tivoli Common Reporting et IBM Cloud APM pour activer la connexion unique (SSO) et éviter les requêtes de connexion répétées.

Avant de commencer

Assurez-vous que l'autorisation OpenID Connect (OIDC) est désactivée pour la console Cloud APM. Pour plus d'informations, voir «Désactivation de l'authentification OpenID Connect pour la console Cloud APM», à la page 922.

Pourquoi et quand exécuter cette tâche

Pour configurer SSO entre Tivoli Common Reporting et Cloud APM, vous devez utiliser un serveur LDAP (Lightweight Directory Access Protocol) commun contenant des utilisateurs définis qui peuvent accéder à l'interface utilisateur Cloud APM et qui sont autorisés à exécuter des rapports.

Procédure

Pour activer la connexion unique sur le serveur Tivoli Common Reporting, procédez comme suit :

1. Configurez Tivoli Common Reporting pour utiliser le serveur LDAP commun. Pour plus d'informations, voir Configuration du référentiel LDAP fédéré.
2. Activez SSO sur le serveur où se trouve Tivoli Common Reporting. Pour plus d'informations, voir Configuration de la connexion unique sur le serveur d'applications.
3. Configurez les utilisateurs LDAP qui peuvent accéder à Tivoli Common Reporting et Jazz for Service Management et disposent des droits nécessaires pour exécuter des rapports. Pour plus d'informations, voir Ajout d'utilisateurs à l'aide de la console d'administration WebSphere et Gestion des rôles des utilisateurs et des groupes.

Sur le serveur Cloud APM, procédez comme suit :

4. Configurez le serveur Cloud APM pour utiliser le serveur LDAP commun si LDAP n'est pas déjà configuré. Pour plus d'informations, voir «Intégration à LDAP», à la page 931.
5. Mettez à jour le domaine Cloud APM dans les fichiers suivants pour vous assurer qu'il correspond au domaine Tivoli Common Reporting et Jazz for Service Management (ce dernier peut être personnalisé ; le domaine par défaut est **defaultWIMFileBasedRealm**) :
   - `oauthVariables-onprem.xml`
   - `cscsRoleAdmin.conf` Pour mettre à jour ce fichier, vous devez créer un fichier `cscsRoleAdmin.new`, comme pour la modification d'un utilisateur Administrateur de rôles, comme indiqué dans «Modification de l'utilisateur apmadmin par défaut», à la page 937.
   - `ldapRegistry.xml`
6. Editez le fichier `ltpa.keys` du serveur Cloud APM :
   a. Recherchez le fichier `ltpa.keys` qui se trouve dans *rép_install*`/usr/servers/apmui/resources/security/` et créez une copie de ce fichier.
   b. Ouvrez la copie dans un éditeur de texte et remplacez la ligne `com.ibm.websphere.CreationHost=localhost` par `com.ibm.websphere.CreationHost=`*nom_hôte_serveur_apm_complet*. Exemple : `com.ibm.websphere.CreationHost=apmhost.example.com`
   c. Copiez le fichier `ltpa.keys` modifié dans le serveur Tivoli Common Reporting.

Sur le serveur Tivoli Common Reporting, procédez comme suit :

7. Importez le fichier `ltpa.keys` modifié sur le serveur Tivoli Common Reporting. Le mot de passe du fichier `ltpa.keys` par défaut est `WebAS`. Pour plus d'informations, voir Importation des clés LTPA.
8. Redémarrez Tivoli Common Reporting. Pour plus d'informations, voir Redémarrage des serveurs d'applications Jazz for Service Management.

Sur le serveur Cloud APM, procédez comme suit :

9. Editez le fichier *rép_install*`/wlp/usr/servers/apmui/user-exit.xml`:

- Ajoutez ou mettez à jour la ligne <webAppSecurity ssoRequiresSSL="true" /> pour ajouter ou éditer l'attribut ssoDomainNames=".*domaine_commun*" à l'élément, où *domaine_commun* est le nom de domaine commun au serveur Tivoli Common Reporting et au serveur Cloud APM.

Exemple :

```
<webAppSecurity ssoRequiresSSL="true" ssoDomainNames=".example.com"
/>
```

Assurez-vous que le nom ssoDomainNames=".*domaine_commun*" commence par un point.

Si l'élément **webAppSecurity** existe dans le fichier apmui/server.xml, supprimez-le.

10. Editez le fichier *rép_install*/wlp/usr/servers/uviews/user-exit.xml:
    - Ajoutez ou mettez à jour la ligne <webAppSecurity ssoRequiresSSL="true" postParamSaveMethod="Session" /> pour ajouter ou éditer l'attribut ssoDomainNames=".*domaine_commun*" à l'élément, où *domaine_commun* correspond au nom de domaine utilisé à l'étape précédente.

    Exemple :

    ```
    <webAppSecurity ssoRequiresSSL="true" postParamSaveMethod="Session" ssoDomainNames=".example.com" />
    ```

    Assurez-vous que le nom ssoDomainNames=".*domaine_commun*" commence par un point.Si l'élément **webAppSecurity** existe dans le fichier uviews/server.xml, supprimez-le.
11. Si les valeurs d'expiration de LTPA sont différentes dans *rép_install*/wlp/usr/servers/apmui/server.xml et *rép_install*/wlp/usr/servers/uviews/server.xml, mettez-les à jour afin qu'elles correspondent :
    a. Editez le fichier *rép_install*/wlp/usr/servers/apmui/user-exit.xml de façon à ajouter ou mettre à jour la valeur d'expiration de LTPA pour le serveur apmui. Exemple :

    ```
    <ltpa expiration="200m" />
    ```

    Si l'élément **ltpa** existe dans le fichier apmui/server.xml, supprimez-le.

    b. Editez le fichier *rép_install*/wlp/usr/servers/uviews/user-exit.xml de façon à ajouter ou mettre à jour la valeur d'expiration de LTPA pour le serveur uviews. Exemple :

    ```
    <ltpa expiration="200m" />
    ```

    Si l'élément **ltpa** existe dans le fichier uviews/server.xml, supprimez-le.
12. Importez la clé LTPA du serveur apmui dans le serveur uviews :
    a. Effectuez une copie de sauvegarde de la clé LTPA du serveur uviews dans *rép_install*/wlp/usr/servers/uviews/resources/security/ltpa.keys.
    b. Copiez la clé LTPA du serveur apmui dans le serveur uviews :

    ```
    cp rép_install/wlp/usr/servers/apmui/resources/security/ltpa.keys
     rép_install/wlp/usr/servers/uviews/resources/security/
    ```
13. Redémarrez tous les services Cloud APM à l'aide de la commande **apm restart_all**. Pour plus d'informations, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.

Résultats

La connexion unique est maintenant activée entre Tivoli Common Reporting et Cloud APM.

Intégration à Dashboard Application Services Hub

Intégrez Dashboard Application Services Hub à Cloud APM pour créer une console unique ou vos propres tableaux de bord personnalisés.

Pour plus d'informations sur l'intégration à Dashboard Application Services Hub, voir Intégration à Jazz for Service Management dans la documentationJazz for Service Management.

Configuration de la connexion unique avec Jazz for Service Management version 1.1.2.0 ou ultérieure

Désactivez OIDC, puis configurez Jazz for Service Management version 1.1.2.0 ou ultérieure et IBM Cloud Application Performance Management pour activer la connexion unique (SSO) et éviter les requêtes de connexion répétées.

Pour activer la connexion unique entre Jazz for Service Management version 1.1.2.0 ou ultérieure et Cloud APM, vous devez effectuer les tâches suivantes :

1. Désactivez l'authentification OpenID Connect pour la console Cloud APM.
2. Activez la connexion unique entre Cloud APM et Jazz for Service Management version 1.1.2.0 ou ultérieure.

Désactivation de l'authentification OpenID Connect pour la console Cloud APM

Vous devez désactiver l'authentification OpenID Connect pour la console Cloud APM avant d'activer la connexion unique (SSO) entre Cloud APM et un autre produit IBM nécessitant LTPA pour SSO.

Bien que OIDC ne soit plus utilisé pour l'authentification d'UI après la mise en place de cette procédure, les API RESTful continuent de se fier à OIDC. Les API RESTful n'interfèrent pas avec SSO (voir «Exploration des API», à la page 1115).

Procédure

Procédez comme suit pour désactiver l'authentification OIDC pour la console Cloud APM.

1. Arrêtez tous les serveurs avec la commande `apm stop_all`. Pour plus d'informations, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.
2. Si LDAP est déjà configuré pour Cloud APM, vous devez temporairement modifier le fichier `commonRegistry.xml`, situé dans *rép_install*`/wlp/usr/shared/config/`, afin d'inclure `basicRegistry.xml` à la place de `ldapRegistry.xml` :
   a. Placez en commentaire la ligne qui fait référence au fichier de registre LDAP, de la manière suivante :
      ```
      <!--include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/-->
      ```
   b. Supprimez les balises de commentaire de la ligne qui fait référence au fichier de registre de base, de la manière suivante :
      ```
      <include optional="false" location="${shared.config.dir}/basicRegistry.xml"/>
      ```
3. Modifiez la valeur de l'attribut oauthRealm dans le fichier *rép_install*`/wlp/usr/shared/config/oauthVariables-onprem.xml` de sorte qu'elle corresponde à la valeur de l'attribut realm dans le fichier `basicRegistry.xml`.
4. Pour éditer le fichier *rép_install*`/wlp/usr/servers/apmui/server-oauth2-tai.xml` afin de supprimer temporairement la propriété **systemUser**, procédez comme suit :
   a. Effectuez une copie de sauvegarde du fichier *rép_install*`/wlp/usr/servers/apmui/server-oauth2-tai.xml`.
   b. Ouvrez le fichier *rép_install*`/wlp/usr/servers/apmui/server-oauth2-tai.xml` et recherchez la ligne qui commence par `<properties`. Supprimez la propriété **systemUser**.
5. Editez le fichier *rép_install*`/wlp/usr/servers/apmui/server.xml` et mettez en commentaire cette ligne comme suit :
   ```
   <!--include optional="true" location="server-relying-party.xml"/-->
   ```
6. Editez le fichier *rép_install*`/wlp/usr/servers/apmui/server-itportal.xml` de façon à modifier la ligne suivante :
   ```
   <application type="eba" id="Blaze" name="Blaze"
      location="${server.config.dir}/apps/com.ibm.tivoli.blaze_2.3.0.7.eba">
   ```
   Modifiez la ligne comme suit :

```
<application type="eba" id="Blaze" name="Blaze"
     location="${server.config.dir}/apps/com.ibm.tivoli.blaze_2.3.0.7.ltpasso.eba">
```

7. Editez le fichier *rép_install*/wlp/usr/servers/uviews/server.xml et mettez en commentaire cette ligne comme suit :

   ```
   <!--include optional="true" location="server-relying-party.xml"/-->
   ```

   Vous devez utiliser le format exact illustré ici pour mettre en commentaire l'instruction include pour le fichier server-relying-party.xml.
8. Exécutez la commande suivante à l'aide du mot de passe correct de l'utilisateur **apmadmin** :

   rép_install/ccm/configureConsole_ltpasso.sh **apmadmin** *mot_de_passe*

   Le *mot_de_passe* par défaut est **apmpass**.
9. Si vous avez désactivé LDAP à l'étape 2, à la page 922, réactivez le registre LDAP dans le fichier commonRegistry.xml :
   a. Placez en commentaire la ligne qui fait référence au registre de base, de la manière suivante :

      ```
      <!--include optional="false" location="${shared.config.dir}/basicRegistry.xml"/-->
      ```
   b. Supprimez les balises de commentaire de la ligne qui fait référence au fichier de registre LDAP, de la manière suivante :

      ```
      <include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/>
      ```
10. Si vous avez modifié la valeur de l'attribut oauthRealm à l'étape 3, à la page 922, mettez-la à jour pour qu'elle corresponde à la valeur de l'attribut realm dans le fichier ldapRegistry.xml.
11. Si vous avez supprimé la propriété **systemUser** à l'étape 4, à la page 923, remplacez le fichier *rép_install*/wlp/usr/servers/apmui/server-oauth2-tai.xml actuel par le fichier de sauvegarde que vous avez créé à l'étape 4a.
12. Démarrez tous les serveurs avec la commande apm restart_all. Pour plus d'informations, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.

Résultats

L'authentification OpenID Connect pour la console Cloud APM est maintenant désactivée.

Activation de la connexion unique entre Cloud APM et Jazz for Service Management version 1.1.2.0 ou ultérieure.

Configurez Jazz for Service Management et IBM Cloud Application Performance Management pour activer la connexion unique (SSO) et éviter les requêtes de connexion répétées.

Avant de commencer

Assurez-vous que l'autorisation OpenID Connect (OIDC) est désactivée pour la console Cloud APM. Pour plus d'informations, voir «Désactivation de l'authentification OpenID Connect pour la console Cloud APM», à la page 922.

Pourquoi et quand exécuter cette tâche

Pour configurer SSO entre Jazz for Service Management et Cloud APM, vous devez utiliser un serveur LDAP (Lightweight Directory Access Protocol) commun contenant des utilisateurs définis qui peuvent accéder à la console Cloud APM et qui sont autorisés à afficher les tableaux de bord dans Dashboard Application Services Hub (DASH).

Procédure

Sur le serveur Jazz for Service Management, procédez comme suit pour activer SSO :

1. Configurez Jazz for Service Management version 1.1.2.0 ou suivante pour utiliser le serveur LDAP commun. Pour plus d'informations, voir Configuration du référentiel LDAP fédéré.

2. Activez SSO sur le serveur où se trouve Jazz for Service Management version 1.1.2.0. Pour plus d'informations, voir Configuration de la connexion unique sur le serveur d'applications.
3. Configurez les utilisateurs LDAP qui ont accès à Jazz for Service Management et disposent des droits nécessaires pour afficher les tableaux de bord. Pour plus d'informations, voir Ajout d'utilisateurs à l'aide de la console d'administration WebSphere et Gestion des rôles des utilisateurs et des groupes.

Sur le serveur Cloud APM, procédez comme suit :

4. Configurez le serveur Cloud APM pour utiliser le serveur LDAP commun si LDAP n'est pas déjà configuré. Pour plus d'informations, voir «Intégration à LDAP», à la page 931.
5. Assurez-vous que le domaine Cloud APM correspond au domaine Jazz for Service Management. Le domaine Jazz for Service Management peut être personnalisé. Le domaine par défaut est **defaultWIMFileBasedRealm**. Mettez le domaine à jour dans les fichiers suivants :
   - `oauthVariables-onprem.xml`
   - `cscsRoleAdmin.conf` Pour mettre à jour ce fichier, vous devez créer un fichier `cscsRoleAdmin.new`, comme pour la modification d'un utilisateur Administrateur de rôles, comme indiqué dans «Modification de l'utilisateur apmadmin par défaut», à la page 937.
   - `ldapRegistry.xml`
6. Editez le fichier `ltpa.keys` du serveur Cloud APM :
   a. Recherchez le fichier `ltpa.keys` qui se trouve dans *rép_install*`/usr/servers/apmui/resources/security/` et créez une copie de ce fichier.
   b. Ouvrez la copie dans un éditeur de texte et remplacez la ligne `com.ibm.websphere.CreationHost=localhost` par `com.ibm.websphere.CreationHost=`*nom_hôte_serveur_apm_complet*. Exemple : `com.ibm.websphere.CreationHost=apmhost.example.com`
   c. Copiez le fichier `ltpa.keys` modifié dans le serveur Jazz for Service Management.

Sur le serveur Jazz for Service Management, procédez comme suit :

7. Importez le fichier `ltpa.keys` modifié sur le serveur Jazz for Service Management. Le mot de passe du fichier `ltpa.keys` par défaut est `WebAS`. Pour plus d'informations, voir Importation des clés LTPA.
8. Redémarrez Jazz for Service Management version 1.1.2.0 ou ultérieure. Pour plus d'informations, voir Redémarrage des serveurs d'applications Jazz for Service Management.

Sur le serveur Cloud APM, procédez comme suit :

9. Editez *rép_install*`/wlp/usr/servers/apmui/user-exit.xml` :
   - Ajoutez ou mettez à jour la ligne `<webAppSecurity ssoRequiresSSL="true" />` pour ajouter ou éditer l'attribut `ssoDomainNames=".`*domaine_commun*`"` à l'élément, où *domaine_commun* est le nom de domaine du serveur Jazz for Service Management et du serveur Cloud APM.

   Exemple :

   ```
   <webAppSecurity ssoRequiresSSL="true" ssoDomainNames=".example.com"
   />
   ```

   Assurez-vous que le nom `ssoDomainNames=".`*domaine_commun*`"` commence par un point.Si l'élément `webAppSecurity` existe dans le fichier `apmui/server.xml`, supprimez-le.
10. Editez *rép_install*`/wlp/usr/servers/uviews/user-exit.xml` :
    - Ajoutez ou mettez à jour la ligne `<webAppSecurity ssoRequiresSSL="true" postParamSaveMethod="Session" />` pour ajouter ou éditer l'attribut `ssoDomainNames=".`*domaine_commun*`"` à l'élément, où *domaine_commun* correspond au nom de domaine utilisé à l'étape précédente.

    Exemple :

    ```
    <webAppSecurity ssoRequiresSSL="true" postParamSaveMethod="Session" ssoDomainNames=".example.com" />
    ```

    Assurez-vous que le nom `ssoDomainNames=".`*domaine_commun*`"` commence par un point.

    Si l'élément **webAppSecurity** existe dans le fichier `uviews/server.xml`, supprimez-le.

11. Si les valeurs d'expiration de LTPA sont différentes dans *rép_install*/wlp/usr/servers/apmui/server.xml et *rép_install*/wlp/usr/servers/uviews/server.xml, mettez-les à jour afin qu'elles correspondent :
    a. Editez le fichier *rép_install*/wlp/usr/servers/apmui/user-exit.xml de façon à ajouter ou mettre à jour la valeur d'expiration de LTPA pour le serveur apmui. Exemple :

       ```
       <ltpa expiration="200m" />
       ```

       Si l'élément **ltpa** existe dans le fichier apmui/server.xml, supprimez-le.
    b. Editez le fichier *rép_install*/wlp/usr/servers/uviews/user-exit.xml de façon à ajouter ou mettre à jour la valeur d'expiration de LTPA pour le serveur uviews. Exemple :

       ```
       <ltpa expiration="200m" />
       ```

       Si l'élément **ltpa** existe dans le fichier uviews/server.xml, supprimez-le.
12. Importez la clé LTPA du serveur apmui dans le serveur uviews :
    a. Effectuez une copie de sauvegarde de la clé LTPA du serveur uviews dans *rép_install*/wlp/usr/servers/uviews/resources/security/ltpa.keys.
    b. Copiez la clé LTPA du serveur apmui dans le serveur uviews :

       ```
       cp rép_install/wlp/usr/servers/apmui/resources/security/ltpa.keys
        rép_install/wlp/usr/servers/uviews/resources/security/
       ```
13. Redémarrez tous les services Cloud APM à l'aide de la commande **apm restart_all**. Pour plus d'informations, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.

Résultats

La connexion unique est maintenant activée entre Jazz for Service Management version 1.1.2.0 ou ultérieure et Cloud APM.

Configuration de l'intégration de console

Pour afficher des contenus externes provenant de la console Cloud APM dans la console Dashboard Application Services Hub, vous pouvez configurer une nouvelle intégration de console.

Pour plus d'informations sur la configuration d'une nouvelle intégration de console, voir Configuration d'une nouvelle intégration de console dans la documentation Jazz for Service Management(https://www.ibm.com/support/knowledgecenter/SSEKCU_1.1.3.0/com.ibm.psc.doc/iscdoc/doc/create_console_integration.html).

Remarque :

- N'utilisez pas l'URL d'intégration de la console par défaut comme indiqué dans la documentation Jazz for Service Management. Utilisez l'URL d'intégration de console suivante pour Cloud APM : http://*nom_hôte_APM_complet*:9443/rest
- La page Contrôle d'accès basé sur les rôles ne peut pas être utilisée lorsque la console Cloud APM est consultée dans la console Dashboard Application Services Hub.
- La page Synthetic Script Manager ne peut pas être utilisée lorsque la console Cloud APM est consultée dans la console Dashboard Application Services Hub.

Connexion au fournisseur de données IBM Cloud Application Performance Management

Pour afficher les données Cloud APM dans la console Dashboard Application Services Hub, vous devez vous connecter au fournisseur de données Cloud APM.

Pour plus d'informations sur la création d'une connexion avec un fournisseur de données distant, voir Création d'une connexion dans la documentation Jazz for Service Management (http://www.ibm.com/support/knowledgecenter/SSEKCU_1.1.2.1/com.ibm.psc.doc/tip_original/cmdoc/connection_creating.html).

Pour plus d'informations sur les détails à spécifier lors de la création d'une connexion, voir la section relative à la configuration de Cloud APM et DASH dans le fichier PDF *Creating custom monitoring dashboards*, disponible à partir du site Application Performance Management Developer Center(https://developer.ibm.com/apm/docs/product-integration/dash-custom-dashboards/).

Création de tableaux de bord personnalisés avec des données IBM Cloud Application Performance Management

Pour afficher des données Cloud APM dans la console Dashboard Application Services Hub, vous pouvez créer des tableaux de bord personnalisés.

Les informations du PDF relatif à *création de tableaux de bords de surveillance de base personnalisés* permettent de configurer des widgets DASH pour récupérer des données des agents Cloud APM. Voir DASH custom dashboards sur APM Developer Center.

Vous trouverez plus d'informations sur la création de tableaux de bord personnalisés et l'ajout de widgets sur la page Working with dashboards or pages de la documentation Jazz for Service Management.

Lorsque vous créez des widgets avec des attributs provenant des agents Cloud APM, vous pouvez voir les attributs d'un agent, mais tous ne sont pas disponibles pour l'affichage dans le tableau de bord. Si aucune donnée n'est affichée à partir d'un attribut dans le widget, c'est peut-être parce que vous avez indiqué un attribut ou un ensemble de données non pris en charge. Pour afficher la liste des attributs qui sont appropriés à l'inclusion dans le widget, suivez la procédure ci-dessous. Connectez vous à console Cloud APM. Sélectionnez **Performance** > **Tableau de bord de performance d'application**. Descendez dans la hiérarchie du tableau de bord jusqu'à une instance d'agent. Cliquez sur l'onglet **Détails d'attribut**. Pour voir quels attributs sont disponibles, créez un tableau avec l'ensemble de données que vous souhaitez utiliser dans votre widget Dashboard Application Services Hub.

Le fournisseur de données Cloud APM peut être utilisé avec les widgets Dashboard Application Services Hub suivants :

- Widget de liste
- Tableau simple
- Graphiques circulaires à jauges :
  - Jauge analogique
  - Jauge de statut
  - Jauge de statut de valeur d'indicateur de volume
- Graphiques :
  - A barres
  - Histogrammes
  - Linéaires
  - A secteurs

Lors de la configuration d'un widget DASH pour récupérer des données de mesure Cloud APM, vous devez indiquer un nom de système géré ou un identifiant de groupe de ressources système. Lorsque vous indiquez un identifiant de groupe de ressources système pour votre widget DASH, la liste des membres du groupe s'affiche. Sélectionnez les agents dont vous souhaitez récupérer les données.

Remarque : Vous ne pouvez pas spécifier les noms des groupes de ressources personnalisées.

Pour l'identifiant de groupe de ressources système, vous ne pouvez pas indiquer le nom que vous voyez dans le Gestionnaire de groupes de ressources. A la place, vous devez indiquer l'identifiant interne du groupe de ressources système. Pour identifier ce dernier, faites une requête via l'API Resource Group Management Service pour récupérer les groupes de ressources système. L'identifiant de groupe de ressources système se trouve dans la zone **keyIndexName**, renvoyée par l'API. Pour plus d'informations sur l'API Resource Group Management Service, voir Utilisation de l'API Resource Group Management Service.

Intégration à LDAP

Pour optimiser votre référentiel d'utilisateurs LDAP dans Cloud APM, vous devez intégrer votre serveur LDAP à votre serveur Cloud APM.

Cloud APM utilise le registre de base des profils Liberty de WebSphere Application Server comme méthode par défaut pour l'authentification des utilisateurs. Vous pouvez également utiliser un registre LDAP pour l'authentification des utilisateurs.

Lorsque vous intégrez Cloud APM à LDAP, vous pouvez utiliser le mode SSL ou non SSL. Procédez comme suit pour intégrer Cloud APM à LDAP :

- Créez une copie des fichiers suivants :
  - *rép_install*/wlp/usr/shared/config/basicRegistry.xml
  - *rép_install*/wlp/usr/shared/config/commonRegistry.xml
  - *rép_install*/wlp/usr/servers/server1/cscs/conf/cscsRoleAdmin.conf
  - *rép_install*/wlp/usr/shared/config/oauthVariables-onprem.xml

  Vous devrez peut-être restaurer ces fichiers plus tard si vous traitez les incidents liés à la configuration, voir «Traitement des incidents liés à la modification de l'utilisateur apmadmin par défaut», à la page 939 et «Traitement des incidents relatifs à la configuration du serveur LDAP», à la page 935.
- (SSL uniquement) Ajoutez le certificat du serveur LDAP.
- «Mise à jour du fichier de registre LDAP», à la page 932.
- Modifiez l'utilisateur apmadmin par défaut.

Ajout du certificat du serveur LDAP

Pour activer les communications SSL entre le serveur Cloud APM et le serveur LDAP, le certificat de signataire du serveur LDAP doit être ajouté à un magasin de clés de confiance sur le serveur Cloud APM.

Avant de commencer

Procurez-vous les certificats de signataire de votre serveur LDAP auprès de l'administrateur LDAP.

Pourquoi et quand exécuter cette tâche

Le certificat de signataire du serveur LDAP doit être ajouté au magasin de clés de confiance référencé par l'attribut **sslAlias** de l'élément <ldapRegistry> dans le fichier ldapRegistry.xml du serveur Cloud APM. Dans la procédure ci-dessous et dans la rubrique des exemples ldapregistry.xml («Exemples ldapregistry.xml», à la page 935) LdapSSLTrustStore.jks est utilisé en tant que nom du magasin de clés de confiance.

Procédure

Suivez la procédure ci-dessous sur le serveur Cloud APM :

1. Accédez au répertoire *rép_install*/wlp/usr/shared/resources/security.

2. Si le fichier *rép_install*/wlp/usr/shared/resources/security/LdapSSLTrustStore.jks existe déjà, renommez-le en LdapSSLTrustStore.jks.sav.
3. Entrez la commande suivante pour créer un nouveau magasin de clés de confiance :

   rép_install/java/bin/keytool -importcert -keystore LdapSSLTrustStore.jks -file *cert.name* -alias ldap

   où *cert.name* est le nom du certificat de signataire du serveur LDAP. Exemple :

   rép_install/java/bin/keytool -importcert -keystore LdapSSLTrustStore.jks -file *ldap-signer.cer* -alias ldap
4. A l'invite, entrez un mot de passe pour le magasin de clés de confiance. Entrez le même mot de passe que celui utilisé pour le magasin de clés de confiance partagé (trust.jks) de Cloud APM. Le mot de passe par défaut est ccmR0cKs!.
5. Lorsque le certificat est affiché et que vous êtes invité à confirmer que vous faites confiance au certificat, entrez Yes.
6. Vous pouvez en vérifier le contenu à l'aide de la commande suivante qui affiche la liste des certificats :

   rép_install/java/bin/keytool -list -v -keystore LdapSSLTrustStore.jks

Résultats

Vous avez ajouté le certificat du serveur LDAP au magasin de clés de confiance partagé.

Que faire ensuite

Maintenant que vous avez ajouté le certificat de signataire du serveur LDAP à un magasin de clés de confiance, vous devez mettre à jour le fichier de registre LDAP comme indiqué dans «Mise à jour du fichier de registre LDAP». La rubrique «Exemples ldapregistry.xml», à la page 935 indique comment spécifier les attributs ssl pour référencer le magasin de clés de confiance que vous venez de créer.

Mise à jour du fichier de registre LDAP

Pour configurer Cloud APM afin qu'il utilise LDAP pour l'authentification d'utilisateur, mettez à jour le fichier ldapRegistry.xml avec les informations sur votre serveur LDAP, puis mettez à jour le fichier commonRegistry.xml afin qu'il renvoie au fichier ldapRegistry.xml.

Avant de commencer

Si SSL est utilisé pendant la configuration, le certificat de signataire du serveur LDAP doit être ajouté au serveur Cloud APM pour permettre la communication SSL entre Cloud APM et LDAP.

Procédure

1. Mettez à jour le fichier ldapRegistry.xml dans le répertoire *rép_install*/wlp/usr/shared/config/. Choisissez le modèle non SSL ou SSL. Ils sont tous les deux identiques, à l'exception des paramètres SSL supplémentaires. Les modèles sont disponibles dans «Exemples ldapregistry.xml», à la page 935. La liste suivante décrit les zones qui doivent être mises à jour et celles qui devront peut-être être mises à jour en fonction de votre environnement :

   Zones qui doivent être mises à jour pour IBM Tivoli Directory Server

   - realm – Il peut s'agir de n'importe quel nom sans espaces ou caractères spéciaux. Le même nom realm est spécifié dans les fichiers ldapRegistry.xml et oauthVariables-onprem.xml.
   - host – Nom d'hôte ou adresse IP du serveur LDAP.
   - port – Numéro de port du serveur LDAP. Par défaut, le serveur LDAP utilise le port 389 pour le mode non SSL et le port 636 pour le mode SSL.
   - baseDN - Emplacement de début de requête dans l'arborescence LDAP.

- `bindDN` – Nom distinctif qualifié complet qui possède les droits pour se lier à votre serveur LDAP et exécuter les requêtes demandées. Si votre serveur LDAP autorise les requêtes anonymes, cette zone n'est pas obligatoire.
- `bindPassword` - Mot de passe pour bindDN. Si votre serveur LDAP autorise les requêtes anonymes, cette zone n'est pas obligatoire.

Zones qui devront peut-être être mises à jour pour IBM Tivoli Directory Server (vérifiez auprès de l'administrateur LDAP)

- `userFilter` et `groupFilter` - Vérifiez auprès de l'administrateur LDAP si la classe d'objet pour `userFilter` et `groupFilter` est correcte.

Zones qui doivent être mises à jour pour Microsoft Active Directory

- `realm` – Il peut s'agir de n'importe quel nom sans espaces ou caractères spéciaux. Le même nom realm est spécifié dans les fichiers `ldapRegistry.xml` et `oauthVariables-onprem.xml`.
- `host` – Nom d'hôte ou adresse IP du serveur LDAP.
- `port` – Numéro de port du serveur LDAP. Par défaut, le serveur LDAP utilise le port 389 pour le mode non SSL et le port 636 pour le mode SSL.
- `baseDN` - Emplacement de début de requête dans l'arborescence LDAP.
- `bindDN` – Nom distinctif qualifié complet qui possède les droits pour se lier à votre serveur LDAP et exécuter les requêtes demandées. Si votre serveur LDAP autorise les requêtes anonymes, cette zone n'est pas obligatoire.
- `bindPassword` – Mot de passe pour `bindDN`. Si votre serveur LDAP autorise les requêtes anonymes, cette zone n'est pas obligatoire.

Zones qui devront peut-être être modifiées pour Microsoft Active Directory (vérifiez auprès de votre administrateur LDAP)

- `userFilter` et `groupFilter` - Vérifiez avec l'administrateur LDAP si la catégorie d'objet pour `userFilter` et `groupFilter` est correcte.

2. (Facultatif) Pour coder la valeur de la propriété `bindPassword` dans le fichier `ldapRegistry.xml`, exécutez securityUtility à partir du répertoire *rép_install*`/wlp/bin`. Entrez le mot de passe `bindPassword` sous la forme d'un argument à partir de la ligne de commande ou lorsque vous y êtes invité. securityUtility génère ensuite la valeur codée. Copiez-la et utilisez-la pour le mot de passe bindPassword dans le fichier `ldapRegistry.xml`.
3. Mettez en commentaire la ligne login property du fichier `ldapRegistry.xml` s'il existe et s'il est activé.
   Active Directory : mettez en commentaire `<loginproperty>sAMAccountName;cn</loginProperty>`
   Tivoli Directory Service : mettez en commentaire `<loginProperty>uid;cn</loginProperty>`
4. (Facultatif) Pour réduire le nombre d'utilisateurs renvoyés par le serveur LDAP, utilisez le paramètre `userFilter`. L'exemple suivant applique un filtre sur l'uid et le département :

```
userFilter="(&amp;(uid=%v)(dept=CNNA)(objectclass=ibmPerson)))"
groupFilter="(&amp;(cn=%v)(objectclass=groupOfUniqueNames))"
userIdMap="*:uid"
groupIdMap="*:cn"
groupMemberIdMap="groupOfNames:member;groupOfUniqueNames:uniqueMember"
```

   L'exemple suivant applique un filtre sur l'uid ou l'adresse e-mail, et le département. Cela signifie que soit l'uid ou le département peut être utilisé dans 'userIdMap' pour la connexion :

```
userFilter="(&amp;((|(emailaddress=%v)(uid=%v))(dept=CNNA)(objectclass=ibmPerson)))"
groupFilter="(&amp;(cn=%v)(objectclass=groupOfUniqueNames))"
userIdMap="*:emailaddress"
groupIdMap="*:cn"
groupMemberIdMap="groupOfNames:member;groupOfUniqueNames:uniqueMember"
```

   L'exemple suivant applique un filtre sur le pays :

```
userFilter="(&amp;(uid=%v)(c=us)(objectclass=ibmPerson)))"
    groupFilter="(&amp;(cn=%v)(objectclass=groupOfUniqueNames))"
    userIdMap="*:uid"
    groupIdMap="*:cn"
    groupMemberIdMap="groupOfNames:member;groupOfUniqueNames:uniqueMember"
```

5. (Facultatif) Pour réduire le nombre d'utilisateurs renvoyés dans les résultats, supprimez la mise en commentaire de la propriété federatedRepository, puis éditez les paramètres **maxSearchResults** et **searchTimeOut**. Si vous ne parvenez pas à éditer le paramètre **maxSearchResults**, le message **Non autorisé** risque de s'afficher si vous tentez d'accéder aux utilisateurs et aux groupes d'utilisateurs dans la fenêtre Contrôle d'accès basé sur les rôles. De plus, MaxResultsExceededException pourrait apparaître dans vos fichiers journaux.
6. Mettez à jour le nom de domaine dans le fichier `oauthVariables-onprem.xml` sous le répertoire `rép_install/wlp/usr/shared/config/` de manière à ce qu'il corresponde au nom realm dans le fichier `ldapregistry.xml`. Par exemple, si le fichier `ldapregistry.xml` a le domaine (realm) suivant : `<ldapRegistry id="ldap" realm="SampleLdapIDSRealm"`, le fichier `oauthVariables-onprem.xml` devrait avoir le même nom de domaine comme suit : `<variable name="oauthRealm" value="SampleLdapIDSRealm" />`.
7. Mettez à jour le fichier `commonRegistry.xml` sous le répertoire *`rép_install`*`/wlp/usr/shared/config/` afin d'utiliser le fichier `ldapRegistry.xml`. Effectuez les opérations suivantes :
   a. Placez en commentaire la ligne qui fait référence au registre de base, de la manière suivante :
      ```
      <!--include optional="false" location="${shared.config.dir}/basicRegistry.xml"/-->
      ```
   b. Supprimez les balises de commentaire de la ligne qui fait référence au fichier de registre LDAP, de la manière suivante :
      ```
      <include optional="false" location="${shared.config.dir}/ldapRegistry.xml"/>
      ```
   c. Sauvegardez le fichier `commonRegistry.xml`.
8. Pour vérifier si la configuration est terminée, accédez à https://*nomhôte*:9443 et essayez de vous connecter avec le compte utilisateur LDAP qui sera le nouvel Administrateur de rôles.
   - Si le message suivant s'affiche, la configuration de votre serveur LDAP a réussi :
     ```
     Non autorisé. Vous ne disposez pas
     des droits vous permettant d'afficher cette application.
     Si vous devez y accéder, veuillez envoyer l'URL à laquelle vous tentez d'accéder
     à votre administrateur de surveillance.
     ```

     La dernière étape à compléter consiste à définir le nouveau compte utilisateur Administrateur de rôles à partir du référentiel LDAP comme utilisateur Cloud APM par défaut, voir Modification de l'utilisateur apmadmin par défaut.
   - Si le message suivant s'affiche, la configuration de votre serveur LDAP a échoué :
     ```
     login failed
     ```

     Vous devrez peut-être revenir à l'authentification du registre de base et/ou traiter les incidents liés à la configuration du serveur LDAP, voir «Traitement des incidents relatifs à la configuration du serveur LDAP», à la page 935 .

Résultats

Vous venez de configurer Cloud APM de sorte à utiliser LDAP pour l'authentification d'utilisateur.

Que faire ensuite

Une fois que vous avez remplacé le mode d'authentification des utilisateurs par LDAP, vous devez modifier l'utilisateur apmadmin par défaut. Pour l'information sur la modification de l'utilisateur par défaut, voir «Modification de l'utilisateur apmadmin par défaut», à la page 937.

Traitement des incidents relatifs à la configuration du serveur LDAP

Il se peut que vous deviez traiter des incidents relatifs à la configuration du serveur LDAP.

Procédure

1. Si une partie ou la totalité des conditions suivantes sont vérifiées, la configuration de votre serveur LDAP a échoué :
   - Vous pouvez toujours vous connecter en tant qu'apmadmin, ou en tant que l'un des utilisateurs définis dans le registre de base.
   - Vous obtenez l'erreur suivante lorsque vous tentez de vous connecter à https://*nom_hôte*:9443

     `login failed`

   Effectuez les vérifications suivantes :
   - Vérifiez que le fichier `commonRegistry.xml` a été correctement mis à jour pour pointer vers `ldapRegistry.xml`.
   - Vérifiez que l'adresse, le port et les données d'identification de liaison du serveur LDAP sont correctement référencés dans le fichier `ldapRegistry.xml`. Toutes les modifications que vous apportez et sauvegardez prennent effet immédiatement.
   - Vérifiez que l'identifiant correct est utilisé dans le fichier `ldapRegistry.xml`. En général, l'`uid` (numéro d'identification utilisateur) de Tivoli Director Server ou le `sAMAccountName` de Microsoft Active Directory se présente sous la forme d'une chaîne unique sans espaces, et est différent du CN. Par exemple, un utilisateur appelé `John Smith` peut avoir le numéro d'identification utilisateur `johnsmith`. Les fichiers exemples `ldapRegistry.xml` sont configurés pour utiliser l'`uid` ou le `sAMAccountName` comme identifiant de connexion. Toutefois, une fois connecté, le premier CN est utilisé pour afficher le nom d'utilisateur.
2. S'il vous faut repasser à basicRegistry, suivez la procédure du document : «Retour de LDAP à basicRegistry», à la page 938.

Exemples ldapregistry.xml

Consultez les exemples de registre LDAP des configurations SSL et non-SSL d'IBM Tivoli Directory Server et de Microsoft Active Directory.

Exemple SSL pour IBM Tivoli Directory Server

```
<server>
  <ldapRegistry id="ldap" realm="SampleLdapIDSRealm"
                host="ldapserver.mycity.mycompany.com" port="636" ignoreCase="true"
                baseDN="o=mycompany,c=us"
                ldapType="IBM Tivoli Directory Server"
                recursiveSearch="true"
                sslEnabled="true" sslRef="LDAPSSLSettings">

    <idsFilters userFilter="(&amp;(uid=%v)(objectclass=ePerson))"
                groupFilter="(&amp;(cn=%v)(|(objectclass=groupOfNames)
                            (objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))"
                userIdMap="*:uid"
                groupIdMap="*:cn"
                groupMemberIdMap="mycompany-allGroups:member;mycompany-allGroups:uniqueMember;
                                  groupOfNames:member;groupOfUniqueNames:uniqueMember">
    </idsFilters>

    <!-- Set up mapping between uid and cn -->
    <!--loginProperty>uid;cn</loginProperty-->

   </ldapRegistry>

   <!-- SSL Settings -->

  <ssl id="LDAPSSLSettings" keyStoreRef="defaultKeyStore" trustStoreRef="LDAPTrustStore"/>
  <keyStore id="LDAPTrustStore" location="${shared.resource.dir}/security/LdapSSLTrustStore.jks"
        password="${trust.store.password}" type="JKS"/>

<!-- Max entries and timeout (in milliseconds) -->
```

```
   <!--federatedRepository maxSearchResults="4500" -->

</server>
```

Exemple non SSL pour IBM Tivoli Directory Server

```
<server>
  <ldapRegistry id="ldap" realm="SampleLdapIDSRealm"
                host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
                baseDN="o=mycompany,c=us"
                ldapType="IBM Tivoli Directory Server"
                recursiveSearch="true">

    <idsFilters userFilter="(&amp;(uid=%v)(objectclass=ePerson))"
                groupFilter="(&amp;(cn=%v)(|(objectclass=groupOfNames)
                              (objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))"
                userIdMap="*:uid"
                groupIdMap="*:cn"
                groupMemberIdMap="mycompany-allGroups:member;mycompany-allGroups:uniqueMember;
                                  groupOfNames:member;groupOfUniqueNames:uniqueMember">
    </idsFilters>

    <!-- Set up mapping between uid and cn -->
    <!--loginProperty>uid;cn</loginProperty-->

  </ldapRegistry>

  <!-- Max entries and timeout (in milliseconds) -->
  <!--federatedRepository maxSearchResults="4500" -->


</server>
```

Exemple SSL pour Microsoft Active Directory

```
<server>
  <ldapRegistry id="ldap" realm="SampleLdapADRealm"
                host="ldapserver.mycity.mycompany.com" port="636" ignoreCase="true"
                baseDN="dc=adtest,dc=mycity,dc=mycompany,dc=com"
                bindDN="cn=testuser,cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
                bindPassword="testuserpwd"
                ldapType="Microsoft Active Directory"
                recursiveSearch="true"
                sslEnabled="true" sslRef="LDAPSSLSettings">

    <actived Filters userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
                     groupFilter="(&amp;(cn=%v)(objectcategory=group))"
                     userIdMap="user:sAMAccountName"
                     groupIdMap="*:cn"
                     groupMemberIdMap="memberOf:member" >
    </actived Filters>

    <!-- Set up mapping between sAMAccountName and cn -->
    <!--loginProperty>sAMAccountName;cn</loginProperty-->

   </ldapRegistry>

   <!-- SSL Settings -->

  <ssl id="LDAPSSLSettings" keyStoreRef="defaultKeyStore" trustStoreRef="LDAPTrustStore"/>
  <keyStore id="LDAPTrustStore" location="${shared.resource.dir}/security/LdapSSLTrustStore.jks"
        password="${trust.store.password}" type="JKS"/>

   <!-- Max entries and timeout (in milliseconds) -->
   <!--federatedRepository maxSearchResults="4500" -->


</server>
```

Exemple non SSL pour Microsoft Active Directory

```
<server>
  <ldapRegistry id="ldap" realm="SampleLdapADRealm"
                host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
                baseDN="dc=adtest,dc=mycity,dc=mycompany,dc=com"
                bindDN="cn=testuser,cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
                bindPassword="testuserpwd"
                ldapType="Microsoft Active Directory"
                recursiveSearch="true">

    <actived Filters
       userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
       groupFilter="(&amp;(cn=%v)(objectcategory=group))"
       userIdMap="user:sAMAccountName"
       groupIdMap="*:cn"
       groupMemberIdMap="memberOf:member" >
    </actived Filters>

    <!-- Set up mapping between sAMAccountName and cn -->
    <!--loginProperty>sAMAccountName;cn</loginProperty-->

  </ldapRegistry>

  <!-- Max entries and timeout (in milliseconds) -->
  <!--federatedRepository maxSearchResults="4500" -->


</server>
```

Modification de l'utilisateur apmadmin par défaut

L'utilisateur par défaut de Cloud APM est apmadmin et le domaine par défaut est customRealm. Par défaut, apmadmin est membre du rôle Administrateur des rôles.

Pourquoi et quand exécuter cette tâche

Cet utilisateur par défaut est défini dans le fichier `basicRegistry.xml` du dossier *rép_install*`/wlp/usr/shared/config/`. Il se peut que vous deviez modifier l'utilisateur par défaut pour l'une des raisons suivantes :

- Vous remplacez l'authentification des utilisateurs à l'aide du registre de base par une authentification LDAP ou changez de registre LDAP.
- Vous souhaitez utiliser un autre utilisateur qui est défini dans le registre d'utilisateurs.
- Vous souhaitez utiliser un autre nom de domaine dans le registre d'utilisateurs.

Procédure

1. Accédez au répertoire *rép_install*`/wlp/usr/servers/server1/cscs/conf`, puis créez un fichier intitulé `cscsRoleAdmin.new`. N'éditez pas ou ne supprimez pas le fichier `cscsRoleAdmin.conf` directement. Toute modification doit être effectuée en créant un fichier `cscsRoleAdmin.new`.
2. Ajoutez un nouvel utilisateur par défaut à `cscsRoleAdmin.new` à l'aide de la syntaxe similaire à l'exemple suivant (contactez votre administrateur LDAP pour obtenir la syntaxe exacte) :

   `user:`*`ExempleDomaineADLDAP`*`/CN=`*`utilisateurtest`*`,CN=`*`utilisateurs`*`,dc=`*`testad`*`,dc=`*`maville`*`,dc=`*`monentreprise`*`,dc=`*`com`*

   Où :

   user Préfixe.

   ExempleDomaineADLDAP
   Domaine spécifié dans le fichier de configuration de registre (`basicRegistry.xml` ou `ldapRegistry.xml`).

utilisateurtest
: Utilisateur qui remplace apmadmin. Il peut s'agir du compte administrateur LDAP ou de n'importe quel compte utilisateur issu de votre annuaire d'utilisateurs.

La syntaxe est sensible à la casse. Voir l'étape 7.

3. Sauvegardez le fichier `cscsRoleAdmin.new`.
4. Mettez à jour le fichier *rép_install*`/wlp/usr/servers/apmui/server-oauth2-tai.xml` de façon à ajouter l'utilisateur de l'étape 2, à la page 937 :
   a. Recherchez la ligne de propriétés `<properties`, ainsi que sa balise fermante `/>`.
   b. Ajoutez une nouvelle ligne avant la balise fermante `/>` contenant : `systemUser="testuser LDAP distinguished name"` où *testuser* correspond à la chaîne user de l'étape 2, à la page 937, par exemple : `systemUser="CN=testuser,CN=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"`
   Remarque : n'incluez pas le préfixe *user:* ou le nom de domaine spécifié à l'étape 2, à la page 937.
   c. Confirmez que la balise fermante `/>` n'a pas été supprimée, puis sauvegardez et fermez le fichier.
5. Mettez à jour le fichier `install_dir/wlp/usr/shared/config/oauthVariables-onprem.xml` et définissez la valeur de l'attribut *oauthRealm* sur la valeur de la propriété *realm* contenue dans le fichier `install_dir/wlp/usr/shared/config/ldapRegistry.xml`.
6. Redémarrez le serveur Cloud APM à l'aide de la commande suivante dans le répertoire `/user/bin/` :
   `apm restart_all`
7. Pour vérifier que vous avez bien modifié le compte apmadmin par défaut, essayez de vous connecter avec votre nouveau compte utilisateur Administrateur de rôles.
   - Si vous parvenez à vous connecter, vous avez bien modifié le compte apmadmin par défaut.
   - Si vous obtenez le message "`Vous ne disposez pas des droits vous permettant d'afficher cette application. Si vous devez y accéder, veuillez envoyer l'URL à laquelle vous tentez d'accéder à votre administrateur système de surveillance`", vous devrez peut-être revenir à l'utilisateur apmadmin ou traiter les incidents de la modification de l'utilisateur apmadmin. Pour plus d'informations, voir «Traitement des incidents liés à la modification de l'utilisateur apmadmin par défaut», à la page 939.

Résultats

L'intégration de Cloud APM à votre serveur LDAP est à présent terminée.

Retour de LDAP à basicRegistry

Cloud APM utilise le registre de base des profils Liberty de WebSphere Application Server comme méthode par défaut pour l'authentification d'utilisateur.

Procédure

1. Arrêtez tous les composants et les services : `apm stop_all`
2. Ouvrez *rép_install*`/wlp/usr/shared/config/commonRegistry.xml`, mettez en commentaire l'entrée ldapRegistry et supprimez la mise en commentaire de l'entrée basicRegistry, ou bien rétablissez une copie de sauvegarde.
3. Ouvrez *rép_install*`/wlp/usr/shared/config/oauth_variables_onPrem.xml`, puis mettez à jour la valeur **`oauthRealm`** à `CustomRealm`, ou bien rétablissez une copie de sauvegarde.
4. Accédez au répertoire *rép_install*`/wlp/usr/servers/server1/cscs/conf`. Créez un fichier intitulé `cscsRoleAdmin.new`. Ajoutez un utilisateur : `user:customRealm/apmadmin`.

   Remarque : Ne modifiez pas directement le fichier `cscsRoleAdmin.conf`.
5. Démarrez tous les composants et services : `apm start_all`

Traitement des incidents liés à la modification de l'utilisateur apmadmin par défaut

Si vous avez des difficultés à modifier l'utilisateur apmadmin par défaut, vous devrez peut-être revenir à l'utilisateur apmadmin ou traiter les incidents de la configuration.

Avant de commencer

Après avoir modifié l'utilisateur apmadmin par défaut, si l'erreur suivante s'affiche encore :

```
Vous ne disposez pas
des droits vous permettant d'afficher cette application. Si vous
devez y accéder, veuillez envoyer
 l'URL à laquelle vous tentez d'accéder à votre administrateur
système de surveillance
```

Vous devrez traiter les incidents liés à la configuration.

Procédure

1. Examinez le fichier `messages.log` dans le répertoire *rép_install*`/wlp/usr/servers/apmui/logs/` à la recherche d'erreurs de type LDAP. Une recherche du mot 'RBAC2' devrait renvoyer plusieurs entrées avec le Nom distinctif attendu, par exemple :

   ```
   [3/8/16 12:40:17:976 CET] 000028c5 com.ibm.tivoli.ccm.rbac.RBACPermissions E **
   RBAC2: user:LdapRealm/cn=John Smith,dc=ibm,dc=com, /ui/tasks/information, task, view,
   false
   ```

   Dans cet exemple, le Nom distinctif attendu est l'utilisateur : `LdapRealm/cn=John Smith,dc=ibm,dc=com`
2. Vérifiez que l'utilisateur et le nom distinctif spécifiés dans `cscsRoleAdmin.conf` correspondent exactement à votre entrée de serveur LDAP. Si des mises à jour sont nécessaires, créez un fichier `cscsRoleAdmin.new` avec l'entrée appropriée, puis exécutez **`apm restart_all`**.
3. Vérifiez que le domaine spécifié dans le fichier `cscsRoleAdmin.conf` correspond exactement au domaine du fichier `ldapRegistry.xml`. Si des mises à jour sont nécessaires, créez un fichier `cscsRoleAdmin.new` avec l'entrée appropriée, puis exécutez la commande **`apm restart_all`**.
4. Vérifiez que vous avez effectué toutes les étapes décrites dans ces sections, «Ajout du certificat du serveur LDAP», à la page 931 «Mise à jour du fichier de registre LDAP», à la page 932.
5. S'il vous faut revenir à la définition de l'apmadmin comme utilisateur par défaut, vous devez également repasser à l'utilisation de customRealm et basicRegistry. Effectuez les étapes décrites dans «Retour de LDAP à basicRegistry», à la page 938.

Intégration à IBM Agent Builder

Vous pouvez créer, modifier, déboguer et conditionner des agents à l'aide d'Agent Builder qui étend les fonctionnalités de surveillance d'un environnement IBM Tivoli Monitoring ou IBM Cloud Application Performance Management. Un agent personnalisé utilise ces environnements pour surveiller tout type de logiciel interne ou personnalisé.

Pour des détails, voir le document IBM Agent Builder - Guide d'utilisation.

Chapitre 12. Mise à niveau

Mettez à niveau vos serveur Cloud APM, agents et collecteurs de données pour bénéficier des toutes dernières fonctions et fonctionnalités qui sont disponibles dans l'édition en cours.

Mise à niveau de votre serveur

Vous pouvez effectuer une mise à niveau de votre serveur Cloud APM de la version 8.1.3 vers la version 8.1.4 pour accéder aux toutes dernières fonctions et améliorer les performances. Si votre serveur exécute la version 8.1.2, effectuez d'abord la mise à niveau vers la version 8.1.3.

Lors de la mise à niveau de la version 8.1.3 vers 8.1.4, n'oubliez pas que la version 8.1.4 prend en charge deux offres et non plus quatre comme dans la version 8.1.3. L'offre Cloud APM, Base version 8.1.4 inclut maintenant les fonctionnalités d'IBM Monitoring version 8.1.3. L'offre Cloud APM, Advanced inclut maintenant les fonctionnalités des trois autres offres version 8.1.3. Pour la mise à niveau, vous devez utiliser le fichier de l'offre V8.1.4 qui correspond à l'offre installée sur le serveur Cloud APM V8.1.3. Les correspondances entre les offres version 8.1.3 ou antérieure et les offres version 8.1.4 sont décrites en détail dans la section Nouvelle stratégie de marque et simplification du produit présentée dans la rubrique Chapitre 1, «Nouveautés», à la page 1.

Deux méthodes différentes vous permettent d'effectuer une mise à niveau du serveur. Le choix de la méthode dépend de la taille de l'environnement surveillé. La première méthode utilise deux systèmes distincts sur lesquels les étapes de mise à niveau sont réalisées *côte à côte* sur ces systèmes. La seconde méthode est mise en oeuvre sur un seul système exécutant la version 8.1.3 du serveur Cloud APM. Il vous suffit ensuite de mettre ce système à niveau vers la version 8.1.4 du serveur Cloud APM.

Quelle que soit la méthode utilisée, vous devez appliquer le correctif temporaire 10 de Cloud APM V8.1.3 (8.1.3.0-IBM-IPM-IF0010) ou un correctif ultérieur au serveur Cloud APM avant d'effectuer la mise à niveau.

Si votre serveur Cloud APM est connecté à une base de données MongoDB distante, vous devez installer MongoDB V3.2.12 avant de mettre à niveau le serveur Cloud APM.

Après avoir déterminé quelle méthode utiliser pour la mise à niveau, utilisez ces instructions pour définir les procédures à suivre :

- Si vous effectuez une mise à niveau côte à côte du serveur Cloud APM, suivez ces procédures :
  1. Si votre serveur Cloud APM est connecté à une base de données MongoDB distante, installez MongoDB V3.2.12 sur votre système distant. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.
  2. Selon l'emplacement de votre serveur Db2, suivez l'une de ces procédures :
     - Si votre serveur Cloud APM utilise un serveur Db2 local, effectuez les étapes décrites dans «Mise à niveau du serveur côte à côte», à la page 955.
     - Si votre serveur Cloud APM est connecté à un serveur Db2 distant, effectuez les étapes décrites dans «Mise à niveau du serveur connecté à un serveur Db2 distant», à la page 967. Cette procédure fait référence aux étapes décrites dans la rubrique «Mise à niveau du serveur côte à côte», à la page 955.
- Si vous effectuez une mise à niveau du serveur Cloud APM sur le même système, suivez ces procédures :
  1. Si votre serveur Cloud APM est connecté à une base de données MongoDB distante, installez MongoDB V3.2.12 sur votre système distant. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.

© Copyright IBM Corp. 2015, 2018

2. Effectuez les étapes décrites dans «Mise à niveau du serveur sur le même système», à la page 945. Suivez cette procédure lorsque votre serveur Cloud APM est connecté à un serveur Db2 local ou distant.

Remarque : Si vous mettez à niveau votre serveur Cloud APM, vous devez également mettre à niveau vos collecteurs de données. Pour plus d'informations, voir Mise à niveau de vos collecteurs de données.

Installation de MongoDB V3.2.12 sur votre système distant

Si votre serveur Cloud APM V8.1.3 est connecté à une base de données MongoDB distante, vous devez installer MongoDB V3.2.12 avant de mettre à niveau le serveur Cloud APM.

Vous pouvez désinstaller MongoDB V3.x et réinstaller la version 3.2.12 sur le système distant, mais cette procédure exige l'arrêt du serveur Cloud APM. Pour éviter d'arrêter le serveur Cloud APM, vous pouvez installer MongoDB V3.2.12 sur un autre système distant, puis mettre à jour le fichier de sauvegarde utilisé pour mettre à niveau le serveur Cloud APM afin d'inclure les paramètres de connexion de MongoDB V3.2.12.

Réinstallation de MongoDB V3.2.12 sur le système distant existant

Pour installer MongoDB V3.2.12 sur le système distant existant, désinstallez MongoDB V3.x et réinstallez MongoDB V3.2.12 sur le même système distant. Cette procédure vous impose d'arrêter le serveur Cloud APM.

Procédure

Effectuez les étapes suivantes en tant que superutilisateur (root) :

1. Effectuez l'une des procédure suivantes, selon le type de mise à niveau de serveur que vous souhaitez :
   - Si vous envisagez de mettre à niveau le serveur côte à côte, reportez-vous aux étapes 1 à 4, à la page 957 de la rubrique *Mise à niveau du serveur côte à côte*.
   - Si vous envisagez de mettre à niveau le serveur sur un système unique, reportez-vous aux étapes 1 à 4, à la page 947 de la rubrique *Mise à niveau du serveur sur le même système*.
2. Exécutez le script `backup.sh` sans paramètres à partir du répertoire tools sur le système sur lequel le serveur Cloud APM V8.1.3 est installé. Le nom du fichier de sauvegarde est indiqué dans la sortie. Par exemple :

```
[root]# /root/min/tools/backup.sh
Le serveur est configuré avec une base de données DB2 distante.
 Ce script doit en outre être exécuté sur la machine DB2 pour sauvegarder la base de données.
Le fichier journal a été créé à l'emplacement "/opt/ibm/ccm/logs/backup_20160424_005922.log".
Démarrage des composants du serveur IBM Performance Management
 et vérification des mots de passe...
Exécution d'une sauvegarde...
Traitement du composant "install"...
Traitement du composant "oslc"...
Traitement du composant "ccs"...
Traitement du composant "apmui"...
Traitement du composant "spark"...
Traitement du composant "min"...
Traitement du composant "min_config"...
Traitement du composant "cscs"...
Traitement du composant "oidc"...
Traitement du composant "oauth2"...
Traitement du composant "scr"...
Traitement du composant "mongodb"...
Traitement du composant "itmcdp"...
Traitement du composant "supports"...
Traitement du composant "biagent"...
Opération de sauvegarde terminée.
```

```
Démarrage des composants...
Création du fichier de sauvegarde...
Toutes les tâches se sont terminées avec succès. Votre sauvegarde est disponible dans le fichier suivant :
/opt/ibm/backups/backup_20160424_005922.tar
```

Pour plus d'informations sur l'exécution du script de sauvegarde lorsqu'un nom d'utilisateur différent de celui par défaut est configuré pour le nom d'utilisateur de l'administrateur de l'interface utilisateur de Cloud APM, voir l'étape 6 de la rubrique *Mise à niveau du serveur sur le même système*.

3. Arrêtez serveur Cloud APM. Sur la ligne de commande, entrez :

   ```
   apm stop_all
   ```

4. Copiez le fichier de sauvegarde dans le système sur lequel vous planifiez d'installer le serveur Cloud APM V8.1.4.
5. Désinstallez MongoDB V3.x du système distant. Sur la ligne de commande, entrez :

   ```
   opt/ibm/mongodb/bin/uninstall-mongodb.sh
   ```

6. Installez MongoDB V3.2.12 sur le même système sur lequel la version préalable de MongoDB a été installée. Pour des instructions, voir les étapes 1 à 2 de la rubrique *Installation d'une base de données MongoDB distante*.

Résultats

La base de données MongoDB sur le système distant exécute la version 3.2.12.

Que faire ensuite

Mettez à niveau le serveur Cloud APM :

- Si vous mettez à niveau le serveur Cloud APM sur un système unique, commencez par l'étape 5 de la rubrique «Mise à niveau du serveur sur le même système», à la page 945.
- Si vous effectuez une mise à niveau côte à côte du serveur Cloud APM avec un serveur Db2 local, commencez par l'étape 5 de la rubrique «Mise à niveau du serveur côte à côte», à la page 955.
- Si vous effectuez une mise à niveau côte à côte du serveur Cloud APM avec un serveur Db2 distant, commencez par l'étape 2 de la rubrique «Mise à niveau du serveur connecté à un serveur Db2 distant», à la page 967.

Installation de MongoDB V3.2.12 sur un système distant distinct

Vous pouvez installer MongoDB V3.2.12 sur un système distant distinct. Mettez à jour le script de sauvegarde que vous prévoyez d'utiliser pour la mise à niveau du serveur Cloud APM afin d'inclure le nom d'hôte ou l'adresse IP de la nouvelle version de MongoDB. Cette procédure ne vous impose pas d'arrêter le serveur Cloud APM.

Pourquoi et quand exécuter cette tâche

Le système sur lequel vous installez MongoDB ne peut pas être l'un des systèmes suivants :

- Le système sur lequel le serveur Cloud APM V8.1.3 est installé.
- Le système distant qui exécute MongoDB V3.x.
- Le système sur lequel vous planifiez d'installer le serveur Cloud APM V8.1.4.

Procédure

Effectuez les étapes suivantes en tant que superutilisateur (root) :

1. Installez MongoDB V3.2.12 sur un système distant. Suivez les étapes de la rubrique «Installation d'une base de données MongoDB distante», à la page 152.
2. Effectuez l'une des procédure suivantes, selon le type de mise à niveau de serveur que vous souhaitez :

- Si vous envisagez de mettre à niveau le serveur côte à côte, reportez-vous aux étapes 1 à 4, à la page 957 de la rubrique *Mise à niveau du serveur côte à côte*.
- Si vous envisagez de mettre à niveau le serveur sur un système unique, reportez-vous aux étapes 1 à 4, à la page 947 de la rubrique *Mise à niveau du serveur sur le même système*.

3. Exécutez le script `backup.sh` sans paramètres à partir du répertoire tools sur le système sur lequel le serveur Cloud APM V8.1.3 est installé. Le nom du fichier de sauvegarde est indiqué dans la sortie. Par exemple :

```
[root]# /root/min/tools/backup.sh
Le serveur est configuré avec une base de données DB2 distante.
 Ce script doit en outre être exécuté sur la machine DB2 pour sauvegarder la base de données.
Le fichier journal a été créé à l'emplacement "/opt/ibm/ccm/logs/backup_20160424_005922.log".
Démarrage des composants du serveur IBM Performance Management
 et vérification des mots de passe...
Exécution d'une sauvegarde...
Traitement du composant "install"...
Traitement du composant "oslc"...
Traitement du composant "ccs"...
Traitement du composant "apmui"...
Traitement du composant "spark"...
Traitement du composant "min"...
Traitement du composant "min_config"...
Traitement du composant "cscs"...
Traitement du composant "oidc"...
Traitement du composant "oauth2"...
Traitement du composant "scr"...
Traitement du composant "mongodb"...
Traitement du composant "itmcdp"...
Traitement du composant "supports"...
Traitement du composant "biagent"...
Opération de sauvegarde terminée.
Démarrage des composants...
Création du fichier de sauvegarde...
Toutes les tâches se sont terminées avec succès. Votre sauvegarde est disponible dans le fichier suivant :
/opt/ibm/backups/backup_20160424_005922.tar
```

   Pour plus d'informations sur l'exécution du script de sauvegarde lorsqu'un nom d'utilisateur différent de celui par défaut est configuré pour le nom d'utilisateur de l'administrateur de l'interface utilisateur de Cloud APM, voir l'étape 6 de la rubrique *Mise à niveau du serveur sur le même système*.

4. Copiez le fichier de sauvegarde dans le système sur lequel vous planifiez d'installer le serveur Cloud APM V8.1.4.
5. Mettez à jour le fichier de sauvegarde pour utiliser le nom d'hôte ou l'adresse IP de MongoDB V3.2.12 pendant la procédure de mise à niveau.
   a. Accédez au répertoire dans lequel se trouve le fichier de sauvegarde.

      ```
      cd répertoire_avec_votre_fichier_sauvegarde
      ```

   b. Créez un répertoire, `backup.extracted`.

      ```
      mkdir backup.extracted
      ```

   c. Accédez à votre nouveau répertoire.

      ```
      cd backup.extracted
      ```

   d. Extrayez le fichier tar de sauvegarde.

      ```
      tar -xf ../backup_horodatage.tar
      ```

   e. Ouvrez le fichier `./min_config/ibm_min_config_backup.json`.
   f. Dans le fichier JSON, recherchez la ligne contenant le nom d'hôte ou l'adresse IP de votre vase de données MongoDB V3.x.

      ```
      \"service\":\"com.ibm.tivoli.ccm.mongo\",\"name\":\"hostname\",\"value\":\
      "adresse_IP_ou_nom_hôte_MongoDB_V3.x_distante\"
      ```

Conseil : Recherchez le texte `com.ibm.tivoli.ccm.mongo` et avancez votre curseur caractère par caractère jusqu'à ce que vous retrouviez l'adresse IP ou le nom d'hôte de votre base de données MongoDB V3.x.

g. Mettez à jour le nom d'hôte ou l'adresse IP avec la valeur de votre base de données MongoDB V3.2.12. Par exemple :

```
\"service\":\"com.ibm.tivoli.ccm.mongo\",
\"name\":\"hostname\",\"value\":\"mongodb3.example.net\"
```

h. Editez le fichier `./mongodb/mongo.properties`. Remplacez la propriété

```
mongo.hostname=adresse_IP_ou_nom_hôte_MongoDB_V3.x_distante
```

par

```
mongo.hostname=adresse_IP_ou_nom_hôte_MongoDB_V3.x_distante
```

Par exemple :

```
mongo.hostname=mongodb3.example.net
```

i. Créez un fichier de sauvegarde dans le répertoire `backup.extracted`.

```
tar -cf ../backup_horodatage.updated.tar *
```

Résultats

MongoDB V3.2.12 s'exécute sur un autre système distant et le fichier de sauvegarde inclut l'adresse IP ou le nom d'hôte de la nouvelle version de MongoDB.

Que faire ensuite

Mettez à niveau le serveur Cloud APM :

- Si vous mettez à niveau le serveur Cloud APM sur un système unique, commencez par l'étape 5 de la rubrique «Mise à niveau du serveur sur le même système».
- Si vous effectuez une mise à niveau côte à côte du serveur Cloud APM avec un serveur Db2 local, commencez par l'étape 5 de la rubrique «Mise à niveau du serveur côte à côte», à la page 955.
- Si vous effectuez une mise à niveau côte à côte du serveur Cloud APM avec un serveur Db2 distant, commencez par l'étape 2 de la rubrique «Mise à niveau du serveur connecté à un serveur Db2 distant», à la page 967.

Une fois la mise à jour du serveur Cloud APM terminée, vous pouvez désinstaller la version 3.x de MongoDB du système distant. Pour effectuer la désinstallation, entrez ce qui suit sur la ligne de commande :

```
opt/ibm/mongodb/bin/uninstall-mongodb.sh
```

Mise à niveau du serveur sur le même système

Vous pouvez mettre à niveau votre serveur Cloud APM de la V8.1.3 vers la V8.1.4 sur le même système. L'avantage de cette méthode est qu'un deuxième système n'est pas nécessaire pour effectuer la mise à niveau. Les clients qui travaillent dans des environnements de petite taille ou de taille moyenne choisissent généralement cette méthode.

Avant de commencer

- Lorsque vous effectuez la mise à niveau du serveur Cloud APM, le serveur Db2 pour le serveur Cloud APM V8.1.4.0 doit être au même niveau de version que le serveur Db2 utilisé par le serveur Cloud APM V8.1.3. Vérifiez la version Db2 utilisée par le serveur Cloud APM V8.1.3 :
  - Si Db2 est installé sur le même système que le serveur Cloud APM, entrez la commande suivante pour vérifier la version de Db2 :

    ```
    rép_install/db2/V10.5/bin/db2level
    ```

où *rép_install* est le répertoire où Db2 est installé.

– Si Db2 est installé sur un système distant, demandez à l'administrateur Db2 de vérifier la version du serveur Db2.

Important :

Le serveur Db2 pour le serveur Cloud APM V8.1.4 doit être au même niveau de version que le serveur Cloud APM V8.1.3 au cours de la mise à niveau de ce dernier.

Si la version Db2 de votre serveur Cloud APM V8.1.3 est Db2 Advanced Enterprise Server Edition V10.5 groupe de correctifs 9, suivez maintenant les étapes décrites dans la note technique Upgrading your Cloud APM server from V8.1.3 to V8.1.4 when your Db2 server is running V10.5 fix pack 9 pour continuer la mise à niveau du serveur Cloud APM de la version 8.1.3 vers la version 8.1.4.

Si vous souhaitez utiliser Db2 V11.1 pour votre serveur Cloud APM V8.1.4, vous pouvez mettre à niveau votre serveur Db2 vers une version prise en charge de Db2 V11.1 une fois la mise à niveau du serveur Cloud APM terminée. Suivez la procédure décrite dans «Mise à niveau du serveur Db2 vers Db2 Advanced Workgroup Server Edition version 11.1.x», à la page 1089.

- Si votre serveur Cloud APM est connecté à un serveur Db2 distant, Db2 Advanced Workgroup Server Edition V11.1 est pris en charge lors de la mise à niveau de votre serveur Cloud APM de la version 8.1.3 à la version 8.1.4.
- Si votre serveur Cloud APM V8.1.3 est connecté à une base de données MongoDB distante, installez MongoDB V3.2.12. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.
- Si LDAP est activé sur votre serveur Cloud APM V8.1.3 afin d'authentifier les utilisateurs de la console Cloud APM, suivez la procédure ci-dessous sur votre serveur Cloud APM V8.1.3 avant de sauvegarder les données V8.1.3 :
  1. Récupérez la valeur de l'attribut *realm* dans le fichier `rép_install/wlp/usr/shared/config/ldapRegistry.xml`.
  2. Vérifiez la valeur de l'attribut *oauthRealm* dans le fichier `rép_install/wlp/usr/shared/config/oauthVariables-onprem.xml`. Si la valeur de l'attribut *oauthRealm* ne correspond pas à la valeur de l'attribut *realm* dans le fichier `ldapRegistry.xml`, mettez à jour la valeur de l'attribut *oauthRealm* de sorte qu'elle corresponde à la valeur de l'attribut *realm*.
  3. Suivez la procédure ci-dessous pour mettre à jour le fichier `rép_install/wlp/usr/servers/apmui/server-oauth2-tai.xml` afin d'ajouter l'utilisateur à partir du fichier `rép_install/wlp/usr/servers/server1/cscs/conf/cscsRoleAdmin.conf` :
     a. Recherchez la ligne de propriétés **<properties** et identifiez le paramètre **systemUser** ; s'il n'existe pas, vous devrez l'ajouter à l'étape suivante. Identifiez la balise fermante **/>** de la ligne de propriétés.
     b. Ajoutez une nouvelle ligne ou modifiez une ligne existante avant la balise fermante **/>**, comme suit :

        ```
        systemUser="testuser LDAP distinguished name"
        ```

        où *testuser* correspond à la chaîne user du fichier `cscsRoleAdmin.conf`, par exemple :

        ```
        systemUser="CN=testuser,CN=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
        ```

        Remarque : N'incluez pas le user:prefix ou le nom de domaine qui a été spécifié dans `cscsRoleAdmin.conf`.
     c. Confirmez que la balise fermante **/>** n'a pas été supprimée, puis sauvegardez et fermez le fichier.
- Si vous avez modifié le magasin de clés de confiance pour votre serveur Cloud APM V8.1.3, remplacez-le par le mot de passe par défaut avant de procéder à la mise à niveau du serveur. Une fois

cette dernière terminée, vous pouvez rétablir votre mot de passe de magasin de clés de confiance personnalisé. Pour plus de détails, consultez cette procédure décrite dans Changing the password for the shared truststore.

Pourquoi et quand exécuter cette tâche

La mise à niveau de la V8.1.3 du serveur Cloud APM vers la V8.1.4 sur le même système inclut les étapes générales suivantes :

1. Installation de Cloud APM V8.1.3 correctif temporaire 10 (8.1.3.0-IBM-IPM-SERVER-IF0010) ou ultérieur sur votre serveur Cloud APM V8.1.3.
2. Sauvegarde des fichiers de configuration et des données du serveur V8.1.3 correctif temporaire 10 ou ultérieur avec le script de sauvegarde qui fait partie de l'installation du serveur V8.1.3 correctif temporaire 10.
3. Désinstallation de votre serveur Cloud APM V8.1.3. Une fois la désinstallation terminée, supprimez les éventuels répertoires `rép_install/wlp-backup*` ; par exemple : `wlp-backup-02`.
4. Si votre serveur Cloud APM est connecté à un serveur Db2 distant, sauvegardez les bases de données DATAMART, WAREHOUS et SCR32 si ces dernières n'ont pas été sauvegardées récemment. Le script `backup.sh` peut être utilisé pour terminer cette sauvegarde. Exécutez ensuite les commandes pour mettre à jour la base de données SCR sur le serveur Db2.
5. Installez le serveur Cloud APM version 8.1.4 et indiquez que vous effectuez une mise à niveau. Le script d'installation restaure les données et les fichiers de configuration du serveur à partir du fichier de sauvegarde du serveur Cloud APM version 8.1.3.

Procédure

Tout en étant connecté en tant que superutilisateur (root) sur le système où votre serveur serveur Cloud APM V8.1.3 est installé, effectuez les opérations suivantes pour mettre à niveau votre serveur vers la V8.1.4 sur le même serveur :

1. Téléchargez l'image d'installation du serveur Cloud APM version 8.1.4 à partir du site de téléchargement vers l'emplacement de transfert de votre choix. Voir «Téléchargement depuis Passport Advantage», à la page 118.
2. Si vous prévoyez de configurer les images d'agent et/ou l'image de la Passerelle hybride lors de la mise à niveau du serveur, téléchargez les images. Pour plus d'informations, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Extrayez les fichiers d'installation du serveur correspondant à votre offre.

   Dans la version 8.1.4, deux offres sont prises en charge, au lieu de quatre comme dans la version 8.1.3. Ces offres sont les suivantes :

   IBM Cloud Application Performance Management, Advanced Private
   `advanced_8.1.4.0.tar`

   IBM Cloud Application Performance Management, Base Private
   `base_8.1.4.0.tar`

   L'offre IBM Cloud Application Performance Management, Base Private inclut désormais les fonctionnalités de la version 8.1.3 de l'offre IBM Monitoring, et l'offre IBM Cloud Application Performance Management, Advanced Private inclut désormais les fonctions des trois autre offres V8.1.3. Pour la mise à niveau, vous devez utiliser le fichier de l'offre V8.1.4 qui correspond à l'offre installée sur le serveur Cloud APM V8.1.3. Par exemple, si IBM Monitoring a été installé sur le serveur Cloud APM V8.1.3, vous devez utiliser le fichier d'offre du IBM Cloud Application Performance Management, Base Private V8.1.4 pour effectuer la mise à niveau.
4. Installez le correctif version 8.1.3 sur votre serveur Cloud APM version 8.1.3.
   a. Téléchargez la version 8.1.3 correctif temporaire 10 (8.1.3.0-IBM-IPM-SERVER-IF0010) ou un correctif ultérieur depuis IBM Fix Central sur le site de support IBM.

b. Copiez le fichier 8.1.3.0-IBM-IPM-SERVER-IF0010.tar vers votre serveur Cloud APM V8.1.3 et procédez comme suit sur le serveur Cloud APM V8.1.3.
   1) Extrayez le package du correctif :
      ```
      tar xvf 8.1.3.0-IBM-IPM-SERVER-IF0010.tar
      ```
   2) Exécutez le script suivant pour appliquer le correctif :
      ```
      apmpatch.sh
      ```

5. Vérifiez que les droits par défaut sont définis correctement. Ouvrez une invite de commande et entrez umask.

   Une valeur de 0022 est renvoyée si les droits sont définis correctement. Si toute autre valeur est renvoyée, définissez les droits appropriés en entrant la commande suivante :
   ```
   umask 0022
   ```

6. Exécutez la commande suivante en tant que superutilisateur pour sauvegarder l'installation de votre serveur Cloud APM version 8.1.3 correctif temporaire 10 ou ultérieure.
   ```
   rép_install/ccm/backup.sh [-f ~/backup813.tar]
   ```

   où *rép_install* est le répertoire dans lequel vous avez installé le serveur Cloud APM version 8.1.3 correctif temporaire 10. Incluez l'option **-f** si vous voulez indiquer le chemin d'accès et le nom de fichier de la sauvegarde du serveur. Par exemple, ~/backup813.tar est sauvegardé sous la forme /root/backup813.tar. Le chemin d'accès par défaut est /opt/ibm/backups/backup_*aaaammjj_hhmmss*.tar, par exemple, /opt/ibm/backups/backup_20160826_155605.tar.

   Important : Si votre base de données MongoDB était installée sur un système distant, utilisez à la place le fichier de sauvegarde que vous avez créé lorsque vous avez mis à niveau MongoDB. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.

   Si votre serveur version 8.1.3 existant est configuré avec un nom d'utilisateur différent de celui par défaut pour le compte administrateur de l'interface Cloud APM, vous devez exécuter le script **backup.sh** suivant en tant que superutilisateur :
   ```
   rép_install/ccm/backup.sh [-f ~/backup813.tar]
   -u nomadministrateur_interfaceutilisateur -p motdepasse_interfaceutilisateur
   ```

   Par exemple, si le nom d'administrateur de l'interface utilisateur de Cloud APM est uiadmin et que le mot de passe autre que celui par défaut pour cet utilisateur est uiadminpwd, entrez la commande suivante :
   ```
   rép_install/ccm/backup.sh -u uiadmin -p uiadminpwd
   ```

   Remarque :

   - Si vous ne voulez pas que le mot de passe soit visible par d'autres utilisateurs, vous pouvez utiliser des variables d'environnement pour fournir le mot de passe et le nom d'utilisateur en entrant les commandes suivantes :
     ```
     export APMADMIN_USERNAME=uiadmin
     export APMADMIN_PASSWORD=uiadminpwd
     ```

     Ensuite, exécutez le script backup.sh en tant que superutilisateur en entrant la commande suivante :
     ```
     rép_install/ccm/backup.sh [-f ~/backup813.tar]
     ```

     Le nom d'utilisateur et le mot de passe de l'administrateur de l'interface utilisateur de Cloud APM est lu à partir de la sauvegarde pendant la phase de restauration.
   - Si votre serveur Cloud APM est connecté à un serveur Db2 distant, vous pouvez ignorer l'avertissement d'exécuter le script de sauvegarde sur le serveur Db2 distant.

   Les messages de sortie vous indiquent la progression de la sauvegarde, le chemin d'accès et le nom de fichier de sauvegarde une fois l'opération terminée.

7. Désinstallation de votre serveur Cloud APM V8.1.3 :
   a. Exécutez la commande suivante dans le répertoire `/opt/ibm/ccm` (ou `/custom_path/ccm` si vous avez installé le serveur à un autre emplacement) :

      ```
      ./uninstall.sh
      ```

   b. Examinez la liste des offres Cloud APM installées et entrez le numéro qui désinstalle toutes les offres (l'ensemble du produit), ou entrez `q` (quit) pour annuler la désinstallation.
8. Si votre serveur Cloud APM est connecté à un serveur Db2 distant, effectuez les étapes suivantes en tant que superutilisateur :
   a. En tant qu'utilisateur d'instance Db2 `db2apm` sur le système sur lequel Db2 est installé, sauvegardez les bases de données DATAMART, WAREHOUS et SCR32.

      Si l'administrateur de base de données qui gère le serveur Db2 distant ne dispose pas de procédures pour sauvegarder la base de données, exécutez le script de sauvegarde serveur Cloud APM :

      1) Copiez `/tools/backup.sh` à partir de l'image d'installation du serveur Cloud APM V8.1.4 vers le serveur Db2 distant.
      2) En tant que superutilisateur et utilisateur d'instance Db2 `db2apm`, entrez les commandes suivantes sur le serveur Db2 distant :

         ```
         chmod 755 backup.sh
         ./backup.sh [-f ~/backup814.tar]
         ```

         AIX Si votre serveur Db2 s'exécute sous AIX, vous devez exécuter le script `backup.sh` dans l'interpréteur de commandes bash. Si ce dernier n'est pas installé sur votre serveur Db2, téléchargez le rpm for bash à partir du site AIX Toolbox for Linux Applications.

   b. Copiez le script `setup-dbconfig-plateforme_64.bin` à partir du répertoire `packages/SCR` de l'image d'installation du serveur Cloud APM version 8.1.4 dans le système du serveur Db2 distant.
   c. Si vous n'êtes pas déjà connecté en tant que `db2apm`, entrez :

      ```
      su - db2apm
      ```

   d. Exécutez le script `setup_dbconfig-plateforme_64.bin` pour configurer la base de données SCR32, où *plateforme* est AIX ou Linux. Exécutez le script en tant qu'utilisateur d'instance Db2 `db2apm` ayant exécuté le script pendant la création de la base de données SCR v8.1.2. N'exécutez pas le script en tant que superutilisateur.

      ```
      /path/setup-dbconfig-linux_64.bin -i console
      ```

      Suivez les invites de la console :

      1) A l'invite de sélection d'un environnement local, entrez `2` pour sélectionner l'anglais.
      2) Entrez `1` pour accepter le contrat de licence.
      3) Entrez le chemin d'accès absolu au dossier d'installation, ou appuyez sur la touche Entrée pour accepter le chemin par défaut. Le chemin par défaut est le chemin d'installation de `installation-dbconfig` pour la V8.1.3. Ne le modifiez pas, sauf s'il est incorrect. Dans cette procédure, le chemin d'accès est appelé `/opt/ibm/db2/tbsmdb`.
      4) Entrez `1` pour sélectionner `IBM Cloud Application Performance Management (APM)` comme produit utilisant la base de données.
      5) Entrez `1` pour sélectionner `Simple` comme type d'installation à exécuter.
      6) Entrez `2` pour que le programme d'installation ne crée pas le schéma de base de données, notamment les tables, les espaces table et les vues.
      7) Entrez les détails de configuration de la base de données suivants lorsque vous y êtes invité :
         - Nom de la base de données (8 caractères au maximum) (VALEUR PAR DEFAUT : SCR32) : SCR32
         - Nom d'hôte ou adresse IP de la base de données (VALEUR PAR DEFAUT) : *nom_hôte_ou_adresse_IP*

- Port de la base de données (VALEUR PAR DEFAUT : 50000) : *port*
- Chemin de la base de données (Valeur par défaut : <valeur par défaut>) : *chemin_par_défaut*

8) Créez une base de données chiffrée (applicable uniquement sur Db2 for Cloud version 10.5 groupe de correctifs 3 ou ultérieur). Appuyez sur la touche **Enter** et acceptez la sélection par défaut qui s'affiche.

e. Mettez à niveau le schéma de base de données et les routines UDF Java dans la base de données SCR Db2. Entrez :

```
cd chemin_install/tbsmdb/tools/XMLtoolkit/bin
./scr_restore.sh -U db2apm -P passw0rd -n
```

où *chemin_install* correspond au chemin que vous avez entré lors de la configuration de `setup-dbconfig`.

Si vous ne voulez pas que le mot de passe apparaisse sur la ligne de commande, omettez l'indicateur `-P` ; le script vous demande alors le mot de passe. Par exemple :

```
./scr_restore.sh -n
Entrez le mot de passe de la base de données :
```

f. Entrez la commande suivante en tant qu'utilisateur `db2apm` pour chaque base de données afin d'ajuster le pool de mémoire tampon après avoir déterminé la taille de votre environnement.

```
db2 connect to WAREHOUS
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size NBR_PAGES_WAREHOUS
db2 disconnect WAREHOUS
db2 connect to DATAMART
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size NBR_PAGES_DATAMART
db2 disconnect DATAMART
db2 connect to SCR32
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size 5000
db2 alter bufferpool TBSMCFG16KBP IMMEDIATE size 1000
db2 alter bufferpool TBSM4KBP IMMEDIATE size 1000
db2 alter bufferpool TBSM32KBP IMMEDIATE size 1000
db2 alter bufferpool TBSMSCR16KBP IMMEDIATE size NBR_PAGES_SCR32
db2 disconnect SCR32
```

où :

WAREHOUS_PAGE_COUNT est le nombre de pages (taille de page de 8K) de mémoire tampon IBMDEFAULTBP de la base de données WAREHOUS : 50000 pour Petite ; 100000 pour Moyenne ou 200000 pour Grande

DATAMART_PAGE_COUNT est le nombre de pages (taille de page de 8K) de mémoire tampon IBMDEFAULTBP de la base de données DATAMART : 100000 pour Petite ; 200000 pour Moyenne ou 300000 pour Grande

SCR32_PAGE_COUNT est le nombre de pages (taille de page de 16K) de mémoire tampon TBSMSCR16KBP de la base de données SCR32 : 30000 pour Petite ; 50000 pour Moyenne ou 100000 pour Grande

Estimez la taille de votre environnement (Petite, Moyenne ou Grande) d'après le tableau de la configuration requise pour le serveur dans «Configuration matérielle requise pour le serveur Cloud APM», à la page 92.

9. Installez la nouvelle version du serveur Cloud APM, puis restaurez les données et la configuration à partir de la sauvegarde. Effectuez ces sous-étapes en tant que superutilisateur.
   a. Si le système informatique ou la machine virtuelle où vous installez le serveur Cloud APM avec un serveur Db2 local utilise LDAP pour authentifier le superutilisateur ou les utilisateurs Db2 pour votre serveur Cloud APM, vous devez créer des utilisateurs Db2 locaux avant d'installer la version 8.1.4. serveur Cloud APM. Effectuez les étapes 1 à 7 de la section «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.
   b. Lorsque vous mettez à niveau votre serveur Cloud APM de la V8.1.3 vers la V8.1.4, vous devez installer la V8.1.4 dans le même répertoire que celui où le serveur V8.1.3 a été précédemment

installé. Ce chemin d'installation était soit le répertoire /opt/ibm par défaut, soit un répertoire que vous avez choisi. Exécutez la commande ./install.sh pour lancer le script d'installation.

c. Lorsque vous êtes invité à effectuer la mise à niveau à partir d'une installation existante du serveur Cloud APM, entrez 1 (oui).

d. Lorsque vous êtes invité à migrer les données et la configuration du serveur automatiquement ou manuellement, entrez 2 pour une migration manuelle.

e. Lorsque vous êtes invité à indiquer l'emplacement du fichier de sauvegarde, entrez le chemin d'accès et le nom de fichier que vous avez créés à l'étape 6, à la page 948 (par exemple, /opt/ibm/backups/backup_20160826_155605.tar).

f. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser.

g. Une fois que le système vous a demandé si vous souhaitiez configurer les images d'installation de vos agents et l'image d'installation de la Passerelle hybride (si cette dernière est utilisée) pour vous connecter au serveur, entrez 1 (oui) pour configurer les images maintenant ou 2 (non) pour reporter la configuration des images des agents et de la Passerelle hybride.

   Si vous avez entré 1 (oui), vous êtes invité à confirmer les informations suivantes :

   - Le chemin d'accès au répertoire sur le serveur où sont stockées les images d'agent et la Passerelle hybride (si cette dernière est utilisée).
     Les images d'agent et celles de la Passerelle hybride peuvent être montées sur une partition NFS, mais elles doivent être accessibles à l'aide du système de fichiers.
   - Entrez le chemin d'accès au répertoire de stockage des images d'installation de l'agent configuré ou acceptez le répertoire *rép_install*/ccm/depot par défaut.
   - Si vous avez accepté le répertoire par défaut de stockage de l'agent configuré et des images de la Passerelle hybride, le programme d'installation crée le répertoire *rép_install*/ccm/depot de stockage de l'agent configuré et des images de la Passerelle hybride. Toutefois, si vous avez choisi de modifier le répertoire, si le programme d'installation ne parvient pas à créer ce répertoire ou que ce dernier n'est pas accessible en écriture, vous êtes invité à spécifier le répertoire de sortie.

   Si vous avez entré 2 (non), cette étape est ignorée.

h. Lorsque vous êtes invité à entrer le nom d'hôte et l'adresse IP du serveur qui sera utilisé dans un navigateur Web pour se connecter à la console Cloud APM, acceptez les valeurs par défaut ou entrez vos propres valeurs. Il s'agit de l'adresse que les utilisateurs saisissent pour démarrer la console Cloud APM à partir de leurs navigateurs Web, par exemple : https://myserver:9443 ou http://myserver:8080. Vous pouvez modifier l'adresse IP et le nom d'hôte ultérieurement. Voir «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.

i. Si votre serveur Cloud APM est connecté à un serveur Db2 distant, répondez aux invites pour vous connecter à la base de données Db2 distante :

```
Entrez les paramètres de configuration pour établir la connexion
à la base de données DB2 existante.
Entrez le nom d'hôte/l'adresse IP pour l'hôte DB2
ou acceptez la valeur par défaut [10.46.40.100] :
Entrez le numéro de port de l'instance DB2 ou acceptez la valeur par défaut [50000] :
Entrez le mot de passe de l'utilisateur "itmuser" :
Entrez le nom d'instance DB2 distante ou acceptez la valeur par défaut [db2apm] :
Entrez le mot de passe de l'utilisateur d'instance "db2apm" :
```

   Si vous recevez un message indiquant que les noms de base de données Db2 doivent correspondre, acceptez les valeurs par défaut de façon à utiliser les noms de la version 8.1.3 :

```
Entrez le nom de la base de données de cache de mesure ou acceptez la valeur par défaut [WAREHOUS] :
Entrez le nom de la base de données de topologie ou acceptez la valeur par défaut [SCR32] :
Entrez le nom de la base de données Datamart ou acceptez la valeur par défaut [DATAMART] :
```

Remarque : Une fois cette étape terminée, ne restaurez pas le serveur Db2 distant.

Si le programme d'installation détecte dans *rép_install*/ccm/depot des packages de configuration d'agent issus d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé les anciens packages et qu'il a créé les nouveaux packages d'agent. Les anciens packages sont nommés *rép_install*/ccm/depot.old.

Si le programme d'installation détecte dans *rép_install* un répertoire keyfiles issu d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé l'ancien répertoire keyfiles et qu'il en a créé un nouveau. L'ancien répertoire keyfiles est nommé *rép_install*/keyfiles.old.

L'analyse des prérequis de votre environnement commence et prend un moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal expliquant la raison de l'échec, tel qu'un espace disque insuffisant. Vous devez corriger le problème et relancer l'installation. Un prérequis «logiciel» tel qu'une mémoire disponible faible n'entraîne pas l'arrêt de l'installation mais vous devez entrer 1 pour continuer l'installation ou 2 pour l'arrêter.

10. Migrez la configuration de la Passerelle hybride :
    - Pour migrer la Passerelle hybride immédiatement après une restauration, exécutez ces commandes sur le serveur Cloud APM en tant que superutilisateur :
      a. Copiez le fichier config.properties restauré dans le répertoire ccm :

         ```
         cp rép_install/ccm/properties/config.properties.restored rép_install/ccm/properties/
         config.properties
         ```

      b. Mettez à jour les date et heure du fichier config.properties afin de recharger la configuration de toutes les passerelles hybrides déjà en cours d'exécution :

         ```
         touch config.properties
         ```

      c. Copiez le fichier config.properties mis à jour dans le composant Central Configuration Services :

         ```
         cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
         CentralConfigurationServer.war/common/config.properties
         ```

    - Si des configurations ont été effectuées au niveau du système mis à niveau après la restauration, procédez comme suit :
      a. Copiez ces deux lignes à partir du fichier *rép_install*/ccm/properties/config.properties.restored :

         ```
         com.ibm.tivoli.ccm.encryption\:key=
         com.ibm.tivoli.ccm.gaian.connect\:gaianReq=
         ```

      b. Remplacez les mêmes lignes dans *rép_install*/ccm/properties/config.properties par celles que vous venez de copier.

      c. Copiez config.properties dans le composant Central Configuration Services :

         ```
         cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
         CentralConfigurationServer.war/common/config.properties
         ```

    Pour vous assurer que le fichier config.properties sous *rép_install*/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/common/ a bien été remplacé, vérifiez que les date et heure modifiées correspondent aux date et heure en cours.

Résultats

Le programme d'installation effectue la mise à niveau vers la nouvelle version du serveur Cloud APM et restaure les données et la configuration à partir de la sauvegarde du serveur. Cette procédure de mise à niveau peut prendre 1 heure ou davantage selon la taille de votre sauvegarde.

Que faire ensuite

- Si vous utilisez les certificats prêts à l'emploi par défaut pour accéder à la console Cloud APM, vous devez suivre les étapes dans cette note technique V8.1.4 Application Performance Management UI certificates are expiring in upgraded environments pour mettre à jour les certificats par défaut afin qu'ils n'expirent pas en avril 2019.

- Avant d'utiliser laconsole Cloud APM, que vous avez mise à niveau, effacez le cache de votre navigateur Web et redémarrez le navigateur. Effacer le cache évite les problèmes que les nouvelles fonctions de cette mise à jour ont créé dans certaines des interfaces utilisateur.
- Utilisateurs de la Passerelle hybride : lors de la mise à niveau, le script de restauration du serveur ajoute la clé de chiffrement V8.1.4 et les données d'identification gaiandb au fichier config.properties restauré. La Passerelle hybride télécharge ensuite le fichier config.properties et tente d'utiliser la nouvelle clé de chiffrement pour déchiffrer le mot de passe ITM. Cette clé n'ayant pas servi au chiffrement du mot de passe, la tentative de déchiffrement échoue, de même que la connexion à Tivoli Enterprise Portal Server. La solution de contournement à ce problème se présente comme suit :
  1. Après une restauration, le répertoire *rép_install*/ccm/propertiescontient les fichiers config.properties et config.properties.restored.
  2. Pour récupérer la Passerelle hybride immédiatement après une restauration, exécutez ces commandes sur le serveur Cloud APM en tant que superutilisateur :

     ```
     cp rép_install/ccm/properties/config.properties.restored rép_install/ccm/
     properties/config.properties
     ```

     Mettez à jour les date et heure du fichier config.properties afin de recharger la configuration de toutes les passerelles hybrides déjà en cours d'exécution :

     ```
     # touch config.properties
     ```

     ```
     cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
     CentralConfigurationServer.war/common/config.properties
     ```
- Si vous souhaitez utiliser les anciens packages de configuration d'agent issus d'une installation précédente pour effectuer les installations d'agent, effectuez les étapes suivantes :
  1. Accédez au répertoire *rép_install*/ccm.
  2. Supprimez le fichier agentconfig.
  3. Remplacez le nom du fichier agentconfig.old par agentconfig.
- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3, vous devez redéfinir clientAuthentication sur true. Copiez l'élément xml ssl qui contient l'attribut enabledCiphers du fichier *rép_install*/wlp/usr/servers/min/server.xml vers le fichier *rép_install*/wlp/usr/servers/min/user-exit.xml s'il n'existe pas déjà dans le fichier user-exit.xml. Ajoutez ensuite la ligne clientAuthentication="true" après la ligne enabledCiphers dans le fichier user-exit.xml. Supprimez l'élément XML ssl du fichier server.xml. L'exemple de code ci-dessous indique où ajouter la ligne clientAuthentication="true" dans le fichier user-exit.xml.

  ```
  <ssl
  id="defaultSSLConfig"
  sslProtocol="TLSv1.2"
  enabledCiphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
  clientAuthentication="true"
  serverKeyAlias="server_key"
  clientKeyAlias="IBM_Tivoli_Monitoring_Certificate"
  keyStoreRef="defaultKeyStore"/>
  ```
- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3 et que vous avez utilisé les certificats par défaut, redéfinissez le protocole de communication utilisé par les agents du serveur Cloud APM sur HTTPS. Pour obtenir des instructions, voir Configuration du protocole de communications pour les agents de serveur.
- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3 et que vous n'avez pas utilisé les certificats par défaut, procédez comme suit :
  1. Codez le mot de passe du magasin de clés du serveur (xor) que vous avez utilisé lors de la création des certificats pour le serveur Cloud APM V8.1.3 :

     ```
     /opt/ibm/wlp/bin/securityUtility encode
     ```
  2. Copiez l'élément xml keyStore du fichier *rép_install*/ibm/wlp/usr/servers/min/server.xml dans le fichier *rép_install*/wlp/usr/servers/min/user-exit.xml s'il n'existe pas déjà dans le fichier

user-exit.xml. Dans le fichier user-exit.xml, remplacez ensuite la valeur de l'attribut password par le mot de passe que vous venez de coder à l'étape 1, à la page 953. Supprimez l'élément XML keyStore du fichier server.xml.

3. Accédez au répertoire *rép_install*.
4. Supprimez le répertoire keyfiles.
5. Remplacez le nom du fichier keyfiles.old par keyfiles.
6. Mettez à jour les certificats utilisés par les agents de surveillance pour se connecter au serveur Cloud APM afin qu'ils exploitent le nouveau magasin de clés. Pour plus d'informations, voir «Configuration des certificats entre le serveur et les agents», à la page 222.
7. Mettez à jour le protocole de communication et les certificats utilisés par les agents du serveur Cloud APM. Pour obtenir des instructions, voir Configuration du protocole de communications pour les agents de serveur.

- Si le système où vous avez installé le serveur Cloud APM utilise LDAP pour authentifier le superutilisateur ou les utilisateurs Db2 et que vous avez mis à jour les mots de passe de l'utilisateur itmuser et des utilisateurs d'instance Db2 à l'étape 6, exécutez l'étape 10 dans «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.
- Reconfigurez et réinstallez les rapports en effectuant les étapes décrites dans «Configuration de l'image d'installation des rapports», à la page 919 et«Installation des rapports», à la page 920.
- Si vous modifiez le nom d'hôte ou l'adresse IP du serveur Cloud APM et que Db2 a été installé en local et intégré à d'autres produits (comme Tivoli Common Reporting), procédez comme suit :
  1. Effectuez les étapes 6, à la page 924, 7, à la page 924 et 8, à la page 924 décrites dans «Activation de la connexion unique entre Cloud APM et Tivoli Common Reporting», à la page 923.
  2. Décataloguez les anciens noeud de serveur et bases de données de Tivoli Common Reporting :

     ```
     db2 list db|node directory

     (db2 list db2 directory ou db2 list node directory)
     db2 uncatalog node alias_noeud
     db2 uncatalog db alias_bd
     ```

  3. Recataloguez le noeud de serveur et les bases de données de Tivoli Common Reporting en effectuant les étapes décrites dans «Configuration d'une connexion ODBC», à la page 918.
- Contrôlez les paramètres de la base de données WAREHOUS qui ont été appliqués par le processus de restauration.

  ```
  update database config for warehous using DFT_DEGREE any
  update database config for warehous using LOGBUFSZ 1024
  update database config for warehous using LOCKLIST AUTOMATIC
  update database config for warehous using SORTHEAP AUTOMATIC
  update database config for warehous using SHEAPTHRES_SHR AUTOMATIC
  update database config for warehous using NUM_IOCLEANERS AUTOMATIC
  update database config for warehous using NUM_IOSERVERS AUTOMATIC
  update database config for warehous using LOGFILSIZ 4096
  update database config for warehous using LOGPRIMARY 10
  update database config for warehous using DBHEAP AUTOMATIC
  update database config for warehous using LOGSECOND 40
  update database config for warehous using AVG_APPLS AUTOMATIC
  update database config for warehous using logarchmeth1 OFF
  update database config for warehous using logarchmeth2 OFF
  update database config for warehous using DATABASE_MEMORY 250000 AUTOMATIC
  ```

  Puisque Cloud APM ne prend pas en charge l'élagage des journaux de base de données, les paramètres logarchmeth1 et logarchmeth2 sont définis sur OFF. Si vous sauvegardez la base de données d'entrepôt et que votre environnement prend en charge l'élagage des journaux, modifiez ces paramètres.
- La plupart des agents Cloud APM V8.1.3 sont compatibles avec le serveur Cloud APM V8.1.4. Vous devez cependant mettre à niveau les agents suivants après avoir mis à niveau le serveur Cloud APM vers la version 8.1.4.0 :

– Si vous utilisez l'agent Synthetic Playback, vous devez le mettre à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence. Vous devez ensuite appliquer le dernier correctif temporaire du serveur Cloud APM 8.1.4.0, disponible depuis Fix Central.
– Monitoring Agent for WebSphere Applications doit être mis à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence.
– Monitoring Agent for MongoDB doit être mis à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence.

Mise à niveau du serveur côte à côte

La tâche de mise à niveau *côte à côte* est effectuée à l'aide de deux systèmes distincts ; un système exécute la version 8.1.3 du serveur Cloud APM, tandis que l'autre exécute la version 8.1.4 du serveur une fois cette procédure de mise à niveau terminée. Avec cette méthode, la durée d'immobilisation est minimale car la version 8.1.3 du serveur Cloud APM fonctionne sans discontinuer pendant l'installation du nouveau serveur version 8.1.4.

Comme le serveur V8.1.3 est arrêté seulement pendant le basculement vers le nouveau serveur V8.1.4, l'utilisateur connaît une interruption minimale. En cas de problèmes ou d'échec de la mise à niveau, un autre avantage de cette méthode est que vous pouvez continuer d'utiliser la version du serveur Cloud APM précédant la mise à niveau, c'est-à-dire la version 8.1.3. Les clients qui travaillent dans des environnements de surveillance de grande taille choisissent généralement cette méthode.

Avant de commencer

- Avant d'effectuer cette procédure de mise à niveau, vérifiez que deux systèmes sont disponibles, un système exécutant la V8.1.3 du serveur Cloud APM et un système distinct pour effectuer la mise à niveau vers la V8.1.4 du serveur.
- Lorsque vous effectuez la mise à niveau du serveur Cloud APM, le serveur Db2 pour le serveur Cloud APM V8.1.4.0 doit être au même niveau de version que le serveur Db2 utilisé par le serveur Cloud APM V8.1.3. Vérifiez la version Db2 utilisée par le serveur Cloud APM V8.1.3 :
  – Si Db2 est installé sur le même système que le serveur Cloud APM, entrez la commande suivante pour vérifier la version de Db2 :

    ```
    rép_install/db2/V10.5/bin/db2level
    ```

    où *rép_install* est le répertoire où Db2 est installé.
  – Si Db2 est installé sur un système distant, demandez à l'administrateur Db2 de vérifier la version du serveur Db2.

  Important :

  Le serveur Db2 pour le serveur Cloud APM V8.1.4 doit être au même niveau de version que le serveur Cloud APM V8.1.3 au cours de la mise à niveau de ce dernier.

  Si la version Db2 de votre serveur Cloud APM V8.1.3 est Db2 Advanced Enterprise Server Edition V10.5 groupe de correctifs 9, suivez maintenant les étapes décrites dans la note technique Upgrading your Cloud APM server from V8.1.3 to V8.1.4 when your Db2 server is running V10.5 fix pack 9 pour continuer la mise à niveau du serveur Cloud APM de la version 8.1.3 vers la version 8.1.4.

  Si vous souhaitez utiliser Db2 V11.1 pour votre serveur Cloud APM V8.1.4, vous pouvez mettre à niveau votre serveur Db2 vers une version prise en charge de Db2 V11.1 une fois la mise à niveau du serveur Cloud APM terminée. Suivez la procédure décrite dans «Mise à niveau du serveur Db2 vers Db2 Advanced Workgroup Server Edition version 11.1.x», à la page 1089.

- Si LDAP est activé sur votre serveur Cloud APM V8.1.3 afin d'authentifier les utilisateurs de la console Cloud APM, suivez la procédure ci-dessous sur votre serveur Cloud APM V8.1.3 avant de sauvegarder les données V8.1.3 :
  1. Récupérez la valeur de l'attribut *realm* dans le fichier `répertoire_install/wlp/usr/shared/config/ldapRegistry.xml`.
  2. Vérifiez la valeur de l'attribut *oauthRealm* dans le fichier `répertoire_install/wlp/usr/shared/config/oauthVariables-onprem.xml`. Si la valeur de l'attribut *oauthRealm* ne correspond pas à la valeur de l'attribut *realm* dans le fichier `ldapRegistry.xml`, mettez à jour la valeur de l'attribut *oauthRealm* de sorte qu'elle corresponde à la valeur de l'attribut *realm*.
  3. Suivez la procédure ci-dessous pour mettre à jour le fichier `répertoire_install/wlp/usr/servers/apmui/server-oauth2-tai.xml` afin d'ajouter l'utilisateur à partir du fichier `répertoire_install/wlp/usr/servers/server1/cscs/conf/cscsRoleAdmin.conf` :
     a. Recherchez la ligne de propriétés **<properties** et identifiez le paramètre **systemUser** ; s'il n'existe pas, vous devrez l'ajouter à l'étape suivante. Identifiez la balise fermante **/>** de la ligne de propriétés.
     b. Ajoutez une nouvelle ligne ou modifiez une ligne existante avant la balise fermante **/>**, comme suit :

        ```
        systemUser="testuser LDAP distinguished name"
        ```

        où *testuser* correspond à la chaîne user du fichier `cscsRoleAdmin.conf`, par exemple :

        ```
        systemUser="CN=testuser,CN=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
        ```

        Remarque : N'incluez pas le user:prefix ou le nom de domaine qui a été spécifié dans `cscsRoleAdmin.conf`.
     c. Confirmez que la balise fermante **/>** n'a pas été supprimée, puis sauvegardez et fermez le fichier.
- Si votre serveur Cloud APM V8.1.3 est connecté à une base de données MongoDB distante, installez MongoDB V3.2.12. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.
- Si vous avez modifié le magasin de clés de confiance pour votre serveur Cloud APM V8.1.3, remplacez-le par le mot de passe par défaut avant de procéder à la mise à niveau du serveur. Une fois cette dernière terminée, vous pouvez rétablir votre mot de passe de magasin de clés de confiance personnalisé. Pour plus de détails, consultez cette procédure décrite dans Changing the password for the shared truststore.

Pourquoi et quand exécuter cette tâche

Ces étapes supposent que le système exécutant la V8.1.3 du serveur Cloud APM utilise le serveur Db2 local installé par défaut avec le serveur Cloud APM. Si le système serveur Cloud APM version 8.1.3 que vous utilisez est connecté à un serveur Db2 distant, vous devez exécuter les étapes dans la rubrique «Mise à niveau du serveur connecté à un serveur Db2 distant», à la page 967 et exécuter les étapes de cette rubrique. Commencez avec les étapes dans «Mise à niveau du serveur connecté à un serveur Db2 distant», à la page 967. Vous êtes renvoyé aux étapes de cette rubrique.

La procédure de mise à niveau du serveur Cloud APM de la V8.1.3 vers la V8.1.4 sur les deux systèmes implique ces étapes générales :

1. Installation de Cloud APM V8.1.3 correctif temporaire 10 (8.1.3.0-IBM-IPM-SERVER-IF0010) ou ultérieur sur votre serveur Cloud APM V8.1.3.
2. Sauvegarde des fichiers de configuration et des données du serveur V8.1.3 correctif temporaire 10 ou ultérieur avec le script de sauvegarde qui fait partie de l'installation du serveur V8.1.3 correctif temporaire 10.

3. Installez votre serveur Cloud APM V8.1.4 et restaurez les données du serveur Cloud APM V8.1.3 de l'étape 2 ou effectuez une sauvegarde et une restauration automatiques des données du serveur V8.1.3.
4. Arrêtez votre serveur Cloud APM V8.1.3.
5. Réaffectez l'adresse IP ou l'adresse IP et le nom d'hôte du serveur Cloud APM V8.1.3 au serveur Cloud APM V8.1.4.

Si vous utilisez un serveur Db2 distant, la procédure implique les étapes générales suivantes :

1. Installation de Cloud APM V8.1.3 correctif temporaire 10 (8.1.3.0-IBM-IPM-SERVER-IF0010) ou ultérieur sur votre serveur Cloud APM V8.1.3.
2. Sauvegardez vos bases de données Db2 V8.1.3.
3. Définissez la nouvelle base de données SCR V8.1.4.
4. Restaurez les données de la base de données Db2 V8.1.3 vers les nouvelles bases de données V8.1.4.
5. Sauvegardez vos données et fichiers de configuration du serveur Cloud APM V8.1.3 à l'aide du script de sauvegarde intégré à l'installation du serveur V8.1.3 si vous effectuez une sauvegarde manuelle.
6. Installez votre serveur Cloud APM V8.1.4 et restaurez les données du serveur Cloud APM V8.1.3 de l'étape 5 ou effectuez une sauvegarde et une restauration automatiques des données du serveur V8.1.3.
7. Arrêtez votre serveur Cloud APM V8.1.3.
8. Le cas échéant, renommez vos nouvelles bases de données version 8.1.4 en utilisant les noms des bases de données version 8.1.3.
9. Réaffectez l'adresse IP ou l'adresse IP et le nom d'hôte du serveur Cloud APM V8.1.3 au serveur V8.1.4.

Procédure

Procédez comme suit en tant que superutilisateur.

1. Téléchargez l'image d'installation du serveur Cloud APM version 8.1.4 à partir du site de téléchargement vers l'emplacement de transfert de votre choix. Voir «Téléchargement depuis Passport Advantage», à la page 118.
2. Si vous prévoyez de configurer les images d'agent et/ou l'image de la Passerelle hybride lors de la mise à niveau du serveur, téléchargez les images. Pour plus d'informations, voir Chapitre 6, «Instructions de téléchargement», à la page 115.
3. Extrayez les fichiers d'installation du serveur correspondant à votre offre.
4. Installez le correctif version 8.1.3 sur votre serveur Cloud APM version 8.1.3.
   a. Téléchargez la version 8.1.3 correctif temporaire 10 (8.1.3.0-IBM-IPM-SERVER-IF0010) ou un correctif ultérieur depuis IBM Fix Central sur le site de support IBM.
   b. Copiez le fichier `8.1.3.0-IBM-IPM-SERVER-IF0010.tar` vers votre serveur Cloud APM V8.1.3 et procédez comme suit sur le serveur Cloud APM V8.1.3.
      1) Extrayez le package du correctif :
         ```
         tar xvf 8.1.3.0-IBM-IPM-SERVER-IF0010.tar
         ```
      2) Exécutez le script suivant pour appliquer le correctif :
         ```
         apmpatch.sh
         ```
5. Si le système informatique ou la machine virtuelle où vous installez le serveur Cloud APM avec un serveur Db2 local utilise LDAP pour authentifier le superutilisateur ou les utilisateurs Db2 pour votre serveur Cloud APM, vous devez créer des utilisateurs Db2 locaux avant d'installer la version 8.1.4. serveur Cloud APM. Effectuez les étapes 1 à 7 de la section «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.
6. Vérifiez que les droits par défaut sont définis correctement. Ouvrez une invite de commande et entrez `umask`.

Une valeur de 0022 est renvoyée si les droits sont définis correctement. Si toute autre valeur est renvoyée, définissez les droits appropriés en entrant la commande suivante :

```
umask 0022
```

7. A partir du répertoire d'où vous avez extrait les fichiers d'installation, installez la V8.1.4 du serveur Cloud APM sur la machine virtuelle ou le système informatique que vous utilisez pour la mise à niveau.
   a. Notez l'emplacement d'installation du serveur V8.1.3 sur le système existant car vous devez installer la V8.1.4 dans le même répertoire sur le système de mise à niveau. Le chemin d'installation était soit le répertoire /opt/ibm par défaut, soit un répertoire que vous avez choisi.
   b. Démarrez le script d'installation :

      ```
      ./install.sh
      ```

8. Après avoir démarré l'installation, lorsque vous êtes invité à effectuer la mise à niveau à partir d'une installation existante du serveur Cloud APM, entrez 1 (oui) pour continuer la mise à niveau.
9. Lorsque vous êtes invité à transférer les données et la configuration du serveur automatiquement ou manuellement à partir du système existant, entrez 1 (oui) pour accepter la valeur par défaut et transférer automatiquement les données, ou entrez 2 (non) pour effectuer une migration manuelle.
   a. Si vous avez entré 2 [manuellement] pour transférer vos données à partir du serveur V8.1.3 existant, vous devez exécuter la sauvegarde en tant que superutilisateur sur ce serveur existant. Le script backup.sh se trouve dans le répertoire ccm du répertoire d'installation du serveur Cloud APM V8.1.3.

      Important : Si votre base de données MongoDB était installée sur un système distant, utilisez à la place le fichier de sauvegarde que vous avez créé lorsque vous avez mis à niveau MongoDB. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.

      Si votre serveur version 8.1.3 existant est configuré avec un nom d'utilisateur différent de celui par défaut pour le compte administrateur de l'interface Cloud APM, vous devez exécuter le script **backup.sh** suivant en tant que superutilisateur :

      ```
      rép_install/ccm/backup.sh [-f ~/backup813.tar]
      -u nomadministrateur_interfaceutilisateur -p motdepasse_interfaceutilisateur
      ```

      Par exemple, si le nom d'administrateur de l'interface utilisateur de Cloud APM est uiadmin et que le mot de passe autre que celui par défaut pour cet utilisateur est uiadminpwd, entrez la commande suivante :

      ```
      rép_install/ccm/backup.sh -u uiadmin -p uiadminpwd
      ```

      Remarque :

      - Si vous ne voulez pas que le mot de passe soit visible par d'autres utilisateurs, vous pouvez utiliser des variables d'environnement pour fournir le mot de passe et le nom d'utilisateur en entrant les commandes suivantes :

        ```
        export APMADMIN_USERNAME=uiadmin
        export APMADMIN_PASSWORD=uiadminpwd
        ```

        Ensuite, exécutez le script backup.sh en tant que superutilisateur en entrant la commande suivante :

        ```
        rép_install/ccm/backup.sh [-f ~/backup813.tar]
        ```

        Le nom d'utilisateur et le mot de passe de l'administrateur de l'interface utilisateur de Cloud APM est lu à partir de la sauvegarde pendant la phase de restauration.
      - Si votre serveur Cloud APM est connecté à un serveur Db2 distant, vous pouvez ignorer l'avertissement d'exécuter le script de sauvegarde sur le serveur Db2 distant.

b. Si vous avez entré 1 [automatiquement] pour transférer vos données à partir du serveur V8.1.3 existant, vous êtes invité à fournir ou à accepter les valeurs par défaut pour configurer la connexion SSH au serveur V8.1.3 existant.

   1) `Entrez le nom du compte administrateur de l'interface utilisateur de Performance Management ou acceptez la valeur par défaut [apmadmin]`
   2) `Entrez le mot de passe du compte administrateur de l'interface utilisateur de Performance Management`
   3) `Entrez le nom d'hôte/l'adresse IP du serveur distant`

   Lorsque vous avez répondu aux invites, une connexion est établie et une sauvegarde des données et de la configuration du serveur existantes est créée. Le temps nécessaire pour créer la sauvegarde est lié à la taille de la sauvegarde.

10. Lorsque la sauvegarde est terminée, vous devez entrer le mot de passe racine du serveur Cloud APM V8.1.4 de manière à pouvoir copier le fichier de sauvegarde sur ce serveur.
11. Si vous migrez manuellement vos données, copiez l'image tar de sauvegarde de l'étape 9 sur le serveur sur lequel vous installez le serveur Cloud APM, puis entrez le chemin d'accès et le nom du fichier que vous avez créé (par exemple, `/opt/ibm/backups/backup_20160826_155605.tar`) lorsque vous y êtes invité.
12. Une fois que le système vous a demandé si vous souhaitiez configurer les images d'installation de vos agents et l'image d'installation de la Passerelle hybride (si cette dernière est utilisée) pour vous connecter au serveur, entrez 1 (oui) pour configurer les images maintenant ou 2 (non) pour reporter la configuration des images des agents et de la Passerelle hybride.

    Si vous avez entré 1 (oui), vous êtes invité à confirmer les informations suivantes :

    - Le chemin d'accès au répertoire sur le serveur où sont stockées les images d'agent et la Passerelle hybride (si cette dernière est utilisée).
      Les images d'agent et celles de la Passerelle hybride peuvent être montées sur une partition NFS, mais elles doivent être accessibles à l'aide du système de fichiers.
    - Entrez le chemin d'accès au répertoire de stockage des images d'installation de l'agent configuré ou acceptez le répertoire *rép_install*`/ccm/depot` par défaut.
    - Si vous avez accepté le répertoire par défaut de stockage de l'agent configuré et des images de la Passerelle hybride, le programme d'installation crée le répertoire *rép_install*`/ccm/depot` de stockage de l'agent configuré et des images de la Passerelle hybride. Toutefois, si vous avez choisi de modifier le répertoire, si le programme d'installation ne parvient pas à créer ce répertoire ou que ce dernier n'est pas accessible en écriture, vous êtes invité à spécifier le répertoire de sortie.

    Si vous avez entré 2 (non), cette étape est ignorée.
13. Lorsque vous êtes invité à entrer le nom d'hôte et l'adresse IP du serveur qui sera utilisé dans un navigateur Web pour se connecter à la console Cloud APM, acceptez les valeurs par défaut ou entrez vos propres valeurs. Il s'agit de l'adresse que les utilisateurs saisissent pour démarrer la console Cloud APM à partir de leurs navigateurs Web, par exemple : `https://myserver:9443` ou `http://myserver:8080`. Vous pouvez modifier l'adresse IP et le nom d'hôte ultérieurement. Voir «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.

Important : Ces étapes supposent que le système du serveur Cloud APM à partir duquel vous effectuez la mise à niveau utilise le serveur Db2 local qui est installé par défaut en même temps que le serveur. Si cette version du serveur est connectée à un serveur Db2 distant, au cours de l'installation de la V8.1.4, vous êtes invité à effectuer les étapes de la rubrique «Mise à niveau du serveur connecté à un serveur Db2 distant», à la page 967 pour sauvegarder les bases de données séparément pour éviter tout problème entre le serveur V8.1.3 et le nouveau serveur V8.1.4.
L'installation du serveur Cloud APM V8.1.4 démarre.

Si le programme d'installation détecte dans *rép_install*/ccm/depot des packages de configuration d'agent issus d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé les anciens packages et qu'il a créé les nouveaux packages d'agent. Les anciens packages sont nommés *rép_install*/ccm/depot.old.

Si le programme d'installation détecte dans *rép_install* un répertoire keyfiles issu d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé l'ancien répertoire keyfiles et qu'il en a créé un nouveau. L'ancien répertoire keyfiles est nommé *rép_install*/keyfiles.old. L'analyse des prérequis de votre environnement commence et prend un moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal expliquant la raison de l'échec, tel qu'un espace disque insuffisant. Vous devez corriger le problème et relancer l'installation. Un prérequis «logiciel» tel qu'une mémoire disponible faible n'entraîne pas l'arrêt de l'installation mais vous devez entrer 1 pour continuer l'installation ou 2 pour l'arrêter.

14. Une fois l'installation terminée, vous pouvez vérifier que la mise à niveau vers la V8.1.4 a réussi en procédant comme suit :
    a. Exécutez la commande **apm status** depuis le répertoire /usr/bin/ sur le serveur V8.1.4 mis à niveau, pour consulter la liste des composants en cours d'exécution. Si tous les composants sont en cours d'exécution, la mise à niveau est réussie.
    b. Si vous vous connectez au Tableau de bord d'Application Performance à l'aide des mêmes données d'identification que celles utilisées pour la V8.1.3 et que vous vérifiez vos applications, groupes et instances pour la V8.1.4, ils sont tels que dans la V8.1.3.
15. Arrêtez le système serveur Cloud APM V8.1.3, s'il fonctionne, en entrant la commande suivante à partir de n'importe quel répertoire :
    ```
    shutdown -P now
    ```
16. Réaffectez l'adresse IP ou l'adresse IP et le nom d'hôte du serveur Cloud APM V8.1.3 au serveur V8.1.4. La réaffectation de l'adresse IP seulement ou de l'adresse IP combinée au nom d'hôte est liée à votre configuration.
    - Si vous utilisez l'adresse IP du serveur Cloud APM pour connecter vos agents à votre serveur, effectuez les étapes décrites dans la rubrique Réaffectation de l'adresse IP du serveur à un autre serveur.
    - Si vous utilisez le nom d'hôte du serveur Cloud APM pour connecter vos agents à votre serveur, effectuez les étapes décrites dans la rubrique Réaffectation de l'adresse IP et du nom d'hôte du serveur à un autre serveur.
17. Migrez la configuration de la Passerelle hybride :
    - Pour migrer la Passerelle hybride immédiatement après une restauration, exécutez ces commandes sur le serveur Cloud APM en tant que superutilisateur :
      a. Copiez le fichier config.properties restauré dans le répertoire ccm :
         ```
         cp rép_install/ccm/properties/config.properties.restored rép_install/ccm/properties/
         config.properties
         ```
      b. Mettez à jour les date et heure du fichier config.properties afin de recharger la configuration de toutes les passerelles hybrides déjà en cours d'exécution :
         ```
         touch config.properties
         ```
      c. Copiez le fichier config.properties mis à jour dans le composant Central Configuration Services :
         ```
         cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
         CentralConfigurationServer.war/common/config.properties
         ```
    - Si des configurations ont été effectuées au niveau du système mis à niveau après la restauration, procédez comme suit :
      a. Copiez ces deux lignes à partir du fichier *rép_install*/ccm/properties/config.properties.restored :
         ```
         com.ibm.tivoli.ccm.encryption\:key=
         com.ibm.tivoli.ccm.gaian.connect\:gaianReq=
         ```

b. Remplacez les mêmes lignes dans *rép_install*/ccm/properties/config.properties par celles que vous venez de copier.

c. Copiez config.properties dans le composant Central Configuration Services :

```
cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
CentralConfigurationServer.war/common/config.properties
```

Pour vous assurer que le fichier config.properties sous *rép_install*/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/common/ a bien été remplacé, vérifiez que les date et heure modifiées correspondent aux date et heure en cours.

Résultats

La mise à niveau du serveur Cloud APM vers la V8.1.4 est terminée. Vous pouvez maintenant accéder aux dernières fonctions pour vos agents et d'autres composants.

Que faire ensuite

- Si vous utilisez les certificats prêts à l'emploi par défaut pour accéder à la console Cloud APM, vous devez suivre les étapes dans cette note technique V8.1.4 Application Performance Management UI certificates are expiring in upgraded environments pour mettre à jour les certificats par défaut afin qu'ils n'expirent pas en avril 2019.
- Avant d'utiliser laconsole Cloud APM, que vous avez mise à niveau, effacez le cache de votre navigateur Web et redémarrez le navigateur. Effacer le cache évite les problèmes que les nouvelles fonctions de cette mise à jour ont créé dans certaines des interfaces utilisateur.
- Si vous souhaitez utiliser les anciens packages de configuration d'agent issus d'une précédente installation pour effectuer les installations d'agent, effectuez les étapes suivantes :
  1. Accédez au répertoire *rép_install*/ccm.
  2. Supprimez le fichier agentconfig.
  3. Remplacez le nom du fichier agentconfig.old par agentconfig.
- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3, vous devez redéfinir clientAuthentication sur true. Copiez l'élément xml ssl qui contient l'attribut enabledCiphers du fichier *rép_install*/wlp/usr/servers/min/server.xml vers le fichier *rép_install*/wlp/usr/servers/min/user-exit.xml s'il n'existe pas déjà dans le fichier user-exit.xml. Ajoutez ensuite la ligne clientAuthentication="true" après la ligne enabledCiphers dans le fichier user-exit.xml. Supprimez l'élément XML ssl du fichier server.xml. L'exemple de code ci-dessous indique où ajouter la ligne clientAuthentication="true" dans le fichier user-exit.xml.

```
<ssl
id="defaultSSLConfig"
sslProtocol="TLSv1.2"
enabledCiphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
clientAuthentication="true"
serverKeyAlias="server_key"
clientKeyAlias="IBM_Tivoli_Monitoring_Certificate"
keyStoreRef="defaultKeyStore"/>
```

- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3 et que vous avez utilisé les certificats par défaut, redéfinissez le protocole de communication utilisé par les agents du serveur Cloud APM sur HTTPS. Pour obtenir des instructions, voir Configuration du protocole de communications pour les agents de serveur.
- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3 et que vous n'avez pas utilisé les certificats par défaut, procédez comme suit :
  1. Codez le mot de passe du magasin de clés du serveur (xor) que vous avez utilisé lors de la création des certificats pour le serveur Cloud APM V8.1.3 :

```
/opt/ibm/wlp/bin/securityUtility encode
```

2. Copiez l'élément xml keyStore du fichier *rép_install*/ibm/wlp/usr/servers/min/server.xml dans le fichier *rép_install*/wlp/usr/servers/min/user-exit.xml s'il n'existe pas déjà dans le fichier user-exit.xml. Dans le fichier user-exit.xml, remplacez ensuite la valeur de l'attribut password par le mot de passe que vous venez de coder à l'étape 1, à la page 961. Supprimez l'élément XML keyStore du fichier server.xml.
3. Accédez au répertoire *rép_install*.
4. Supprimez le répertoire keyfiles.
5. Remplacez le nom du fichier keyfiles.old par keyfiles.
6. Mettez à jour les certificats utilisés par les agents de surveillance pour se connecter au serveur Cloud APM afin qu'ils exploitent le nouveau magasin de clés. Pour plus d'informations, voir «Configuration des certificats entre le serveur et les agents», à la page 222.
7. Mettez à jour le protocole de communication et les certificats utilisés par les agents du serveur Cloud APM. Pour obtenir des instructions, voir Configuration du protocole de communications pour les agents de serveur.

- Si le système où vous avez installé le serveur Cloud APM utilise LDAP pour authentifier le superutilisateur ou les utilisateurs Db2 et que vous avez mis à jour les mots de passe de l'utilisateur itmuser et des utilisateurs d'instance Db2 à l'étape 6, exécutez l'étape 10 dans «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.
- Reconfigurez et réinstallez les rapports en effectuant les étapes décrites dans «Configuration de l'image d'installation des rapports», à la page 919 et«Installation des rapports», à la page 920.
- Si vous modifiez le nom d'hôte ou l'adresse IP du serveur Cloud APM et que Db2 a été installé en local et intégré à d'autres produits (comme Tivoli Common Reporting), procédez comme suit :
  1. Effectuez les étapes 6, à la page 924, 7, à la page 924 et 8, à la page 924 décrites dans «Activation de la connexion unique entre Cloud APM et Tivoli Common Reporting», à la page 923.
  2. Décataloguez les anciens noeud de serveur et bases de données de Tivoli Common Reporting :
     ```
     db2 list db|node directory

     (db2 list db2 directory ou db2 list node directory)
     db2 uncatalog node alias_noeud
     db2 uncatalog db alias_bd
     ```
  3. Recataloguez le noeud de serveur et les bases de données de Tivoli Common Reporting en effectuant les étapes décrites dans «Configuration d'une connexion ODBC», à la page 918.
- La plupart des agents Cloud APM V8.1.3 sont compatibles avec le serveur Cloud APM V8.1.4. Vous devez cependant mettre à niveau les agents suivants après avoir mis à niveau le serveur Cloud APM vers la version 8.1.4.0 :
  – Si vous utilisez l'agent Synthetic Playback, vous devez le mettre à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence. Vous devez ensuite appliquer le dernier correctif temporaire du serveur Cloud APM 8.1.4.0, disponible depuis Fix Central.
  – Monitoring Agent for WebSphere Applications doit être mis à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence.
  – Monitoring Agent for MongoDB doit être mis à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence.

Réaffectation de l'adresse IP et du nom d'hôte du serveur à un autre serveur

Si vous utilisez le nom d'hôte du serveur pour connecter vos agents au serveur Cloud APM, une fois la mise à niveau du serveur terminée, vous devez réaffecter l'adresse IP et le nom d'hôte du serveur Cloud APM V8.1.3 au serveur V8.1.4 mis à niveau.

Dans le cadre de cette réaffectation, vous devez également remplacer le paramètre de nom d'hôte dans la configuration Db2 sur le serveur Cloud APM V8.1.4.

Avant de commencer

Si vous prévoyez d'installer de nouveaux agents après avoir réaffecté l'adresse IP et le nom d'hôte du serveur, créez des packages de configuration pour les images d'agent (voir l'étape 2 dans «Configuration des images téléchargées», à la page 162). Sinon, les agents ne se connecteront pas au serveur Cloud APM ou ne s'afficheront pas dans la console Cloud APM.

Procédure

Effectuez les étapes suivantes en tant que superutilisateur sur le serveur Cloud APM V8.1.4 mis à niveau :

1. Arrêtez tous les composants du serveur en entrant la commande suivante dans le répertoire `/usr/bin` :

   ```
   apm stop_all
   ```

2. Réaffectez l'adresse IP du serveur Cloud APM V8.1.3 au serveur V8.1.4 :
   a. Pour déterminer l'adresse IP et le nombre d'adaptateurs de réseau sur le serveur V8.1.3, exécutez la commande suivante à partir de ce serveur :

      ```
      ip addr
      ```

   b. Pour déterminer l'adresse IP et le nombre d'adaptateurs de réseau sur le nouveau serveur V8.1.4 mis à niveau, exécutez la commande suivante à partir de ce serveur :

      ```
      ip addr
      ```

   c. Si un seul adaptateur de réseau est installé sur le serveur V8.1.3, entrez la commande suivante pour arrêter ce système serveur et libérer l'adresse IP afin de la réutiliser :

      ```
      shutdown -P now
      ```

      Si plusieurs adaptateurs de réseau sont installés sur le serveur V8.1.3, entrez la commande suivante pour arrêter l'adaptateur de réseau configuré avec l'adresse IP sur le serveur et libérer l'adresse IP afin de la réutiliser :

      ```
      ip link set dev ADAPTATEUR down
      ```

      où *ADAPTATEUR* est le nom de l'adaptateur indiqué dans la sous-étape 2a.

   d. Entrez les commandes suivantes sur le serveur V8.1.4 afin de réaffecter l'adresse IP du serveur V8.1.3 au serveur V8.1.4. L'adresse IP du serveur V8.1.3 devient l'adresse IP du serveur V8.1.4 :

      ```
      TEMP=/tmp/adapter.$$
      sed 's/IPADDR=.*$/IPADDR='"IP"'/'
      /etc/sysconfig/network-scripts/ifcfg-ADAPTATEUR >$TEMP
      ```

      où *IP* est l'adresse IP du serveur V8.1.3 et *ADAPTATEUR* le nom de l'adaptateur indiqué dans la sous-étape 2b.

      Entrez la commande suivante pour effectuer la réaffectation :

      ```
      cp $TEMP /etc/sysconfig/network-scripts/ifcfg-ADAPTATEUR
      ```

      Entrez la commande suivante pour redémarrer l'adaptateur de réseau :

      ```
      /etc/init.d/network restart
      ```

   L'adaptateur de réseau V8.1.4 utilise maintenant l'adresse IP V8.1.3 comme son adresse IP.

3. Modifiez l'adresse IP et le nom d'hôte du serveur utilisé pour démarrer la console Cloud APM. Il s'agit de l'adresse que les utilisateurs entrent pour démarrer la console à partir de leurs navigateurs Web, par exemple `https://monserver:9443` ou `http://monserver:8080`. Accédez au répertoire *rép_install*`/ccm` et exécutez la commande suivante :

```
configure_server_address.sh
```

A l'invite du système, entrez le nouveau nom du serveur hôte et la nouvelle adresse IP.

4. Mettez à jour les noms de fichier de l'agent de serveur. Les agents de serveur sont notamment l'agent Synthetic Events, l'agent Transaction Events et éventuellement l'agent Bluemix Integration. Basculez vers le répertoire *rép_install*/serveragents/bin et exécutez la commande suivante :
   ```
   update_config_files.sh
   ```
5. Redéfinissez les références au serveur Cloud APM sur le serveur Db2 sur la nouvelle adresse IP et le nouveau nom d'hôte :
   a. Sur le serveur Cloud APM V8.1.4, mettez à jour la variable de registre *DB2SYSTEM* de sorte qu'elle corresponde au nom d'hôte du serveur Cloud APM V8.1.3 :
      ```
      source /home/db2apm/sqllib/db2profile
      db2set -g DB2SYSTEM=nom_hôte
      ```
      où *nom_hôte* est le nom d'hôte du serveur V8.1.3.
   b. Si votre base de données Db2 se trouve sur un système local, modifiez le nom d'hôte sur le serveur Cloud APM V8.1.4 en éditant le fichier /home/db2apm/sqllib/db2nodes.cfg et en remplaçant le nom d'hôte V8.1.4 par le nom d'hôte du serveur V8.1.3.
   c. Si votre base de données Db2 se trouve sur un système local, mettez à jour le fichier de configuration de l'administrateur Db2 en entrant les commandes suivantes :
      ```
      su - db2apm -c 'db2 update admin cfg using DB2SYSTEM nom_hôte'
      su - db2apm -c 'db2 update admin cfg using SMTP_SERVER nom_hôte'
      ```
      où *nom_hôte* est le nom d'hôte du serveur V8.1.3.
6. Redémarrez les composants serveur en entrant la commande suivante dans le répertoire /usr/bin :
   ```
   apm start_all
   ```
7. Redéfinissez le nom d'hôte du serveur Cloud APM dans le composant Central Configuration Services.
   a. Le cas échéant, connectez-vous à la console Cloud APM. (Voir «Démarrage de la console Cloud APM», à la page 989.)
   b. Cliquez sur **Configuration système** > **Configuration avancée** et **Configuration centrale d'agent**.
   c. Dans la zone **Substitution du nom d'hôte**, entrez la nouvelle adresse IP ou le nom d'hôte complet du serveur Cloud APM.

   Après avoir cliqué sur **Sauvegarder**, le nouveau nom d'hôte est mis à jour dans le composant Central Configuration Services.
8. Sur les systèmes où vos agents sont installés, connectez les agents à la nouvelle adresse IP et au nouveau nom d'hôte du serveur. Voir «Connexion des agents à un autre serveur», à la page 220.
9. Si des packages de rapports pour l'agent Response Time Monitoring et l'agent WebSphere Applications sont installés, vous devez les réinstaller pour les deux agents. Pour plus d'informations, voir «Installation des rapports», à la page 920. Redémarrez le serveur Tivoli Common Reporting, puis effectuez les étapes présentées dans les sous-rubriques sous Redémarrage des serveurs d'applications Jazz for Service Management.

Résultats

Le serveur Cloud APM V8.1.4 devient le nouveau serveur actif.

Réaffectation de l'adresse IP du serveur à un autre serveur

Si vous utilisez l'adresse IP du serveur pour connecter vos agents au serveur Cloud APM, une fois la mise à niveau du serveur terminée, vous devez réaffecter l'adresse IP du serveur Cloud APM V8.1.3 au serveur V8.1.4 mis à niveau pour pointer l'adresse IP V8.1.3 sur le nom d'hôte du serveur V8.1.4.

Important : Cette procédure décrit une méthode de réaffectation de l'adresse IP. Il en existe d'autres. Pour plus d'informations, voir les informations relatives à la configuration réseau à l'aide de l'interface de ligne de commande dans le document Networking Guide de la documentation Red Hat.

Avant de commencer

Si vous prévoyez d'installer de nouveaux agents après avoir réaffecté l'adresse IP du serveur, créez des packages de configuration pour les images d'agent (voir l'étape 2 dans «Configuration des images téléchargées», à la page 162). Sinon, les agents ne se connecteront pas au serveur Cloud APM ou ne s'afficheront pas dans la console Cloud APM.

Procédure

Effectuez les opérations suivantes en tant que superutilisateur (root) :

1. Modifiez l'adresse IP et le nom d'hôte du serveur utilisé pour démarrer la console Cloud APM. Il s'agit de l'adresse que les utilisateurs entrent pour démarrer la console à partir de leurs navigateurs Web, par exemple `https://monserveur:9443` ou `http://monserveur:8080`. Accédez au répertoire *rép_install*`/ccm` et exécutez la commande suivante :

   ```
   configure_server_address.sh
   ```

   A l'invite du système, entrez le nouveau nom du serveur hôte et la nouvelle adresse IP.
2. Mettez à jour les noms de fichier de l'agent de serveur. Les agents de serveur sont notamment l'agent Synthetic Events, l'agent Transaction Events et éventuellement l'agent Bluemix Integration. Basculez vers le répertoire *rép_install*`/serveragents/bin` et exécutez la commande suivante :

   ```
   update_config_files.sh
   ```
3. Réaffectez l'adresse IP du serveur Cloud APM V8.1.3 au serveur V8.1.4 :
   a. Pour déterminer l'adresse IP et le nombre d'adaptateurs de réseau sur le serveur V8.1.3, exécutez la commande suivante à partir de ce serveur :

      ```
      ip addr
      ```
   b. Pour déterminer l'adresse IP et le nombre d'adaptateurs de réseau sur le nouveau serveur V8.1.4 mis à niveau, exécutez la commande suivante à partir de ce serveur :

      ```
      ip addr
      ```
   c. Si un seul adaptateur de réseau est installé sur le serveur V8.1.3, entrez la commande suivante pour arrêter ce système serveur et libérer l'adresse IP afin de la réutiliser :

      ```
      shutdown -P now
      ```

      Si plusieurs adaptateurs de réseau sont installés sur le serveur V8.1.3, entrez la commande suivante pour arrêter l'adaptateur de réseau configuré avec l'adresse IP sur le serveur et libérer l'adresse IP afin de la réutiliser :

      ```
      ip link set dev ADAPTATEUR down
      ```

      où *ADAPTATEUR* est le nom de l'adaptateur indiqué dans la sous-étape 3a.
   d. Entrez les commandes suivantes sur le serveur V8.1.4 afin de réaffecter l'adresse IP du serveur V8.1.3 au serveur V8.1.4. L'adresse IP du serveur V8.1.3 devient l'adresse IP du serveur V8.1.4 :

      ```
      TEMP=/tmp/adapter.$$
      sed 's/IPADDR=.*$/IPADDR='"IP"'/'
      /etc/sysconfig/network-scripts/ifcfg-ADAPTATEUR >$TEMP
      ```

      où *IP* est l'adresse IP du serveur V8.1.3 et *ADAPTATEUR* le nom de l'adaptateur indiqué dans la sous-étape 3b.

      Entrez la commande suivante pour effectuer la réaffectation :

      ```
      cp $TEMP /etc/sysconfig/network-scripts/ifcfg-ADAPTATEUR
      ```

Entrez la commande suivante pour redémarrer l'adaptateur de réseau :

```
/etc/init.d/network restart
```

L'adaptateur de réseau V8.1.4 utilise maintenant l'adresse IP V8.1.3 comme son adresse IP.

4. Sur le serveur V8.1.4, ouvrez le fichier `/etc/hosts` dans un éditeur de texte de votre choix, puis remplacez l'adresse IP en regard du nom d'hôte V8.1.4 par l'adresse IP du serveur V8.1.3.

   Remarque : Si vous avez réaffecté l'adresse IP V8.1.3 au serveur V8.1.4, vous n'avez pas besoin de modifier la configuration DNS du réseau.

5. Redéfinissez le nom d'hôte du serveur Cloud APM dans le composant Central Configuration Services.
   a. Le cas échéant, connectez-vous à la console Cloud APM. (Voir «Démarrage de la console Cloud APM», à la page 989.)
   b. Cliquez sur **Configuration système** > **Configuration avancée** et **Configuration centrale d'agent**.
   c. Dans la zone **Substitution du nom d'hôte**, entrez la nouvelle adresse IP ou le nom d'hôte complet du serveur Cloud APM.

   Après avoir cliqué sur **Sauvegarder**, le nouveau nom d'hôte est mis à jour dans le composant Central Configuration Services.

6. Si des packages de rapports pour l'agent Response Time Monitoring et l'agent WebSphere Applications sont installés, vous devez les réinstaller pour les deux agents. Pour plus d'informations, voir «Installation des rapports», à la page 920. Redémarrez le serveur Tivoli Common Reporting, puis effectuez les étapes présentées dans les sous-rubriques sous Redémarrage des serveurs d'applications Jazz for Service Management.

7. Facultatif : A tout moment, si vous avez besoin de restaurer les adresses IP d'origine des serveurs existants V8.1.3 et des serveurs mis à niveau V8.1.4, procédez comme suit :
   a. Pour restaurer l'adresse IP d'origine du serveur V8.1.4, exécutez les commandes suivantes :

      ```
      TEMP=/tmp/adapter.$$
      sed 's/IPADDR=.*$/IPADDR='"IP"'/'
      /etc/sysconfig/network-scripts/ifcfg-ADAPTATEUR >$TEMP
      ```

      Remplacez l'adresse *IP* dans la commande précédente par l'adresse IP d'origine du serveur V8.1.4 en cours de restauration, puis remplacez *ADAPTATEUR* par le nom de l'adaptateur indiqué à l'étape précédente 3. b.

      Entrez la commande suivante pour effectuer la réaffectation :

      ```
      cp $TEMP /etc/sysconfig/network-scripts/ifcfg-ADAPTATEUR
      ```

      Exécutez cette commande pour redémarrer l'adaptateur de réseau V8.1.4 :

      ```
      /etc/init.d/network restart
      ```

   b. Si un seul adaptateur de réseau est installé sur le système du serveur V8.1.3 et que le système a été arrêté, vous devez redémarrer le système. Si vous utilisez un système virtuel, vous devez utiliser le logiciel d'administration virtuel pour redémarrer le système. Si vous utilisez un système physique, vous devez le localiser et le remettre sous tension.

      Si plusieurs adaptateurs de réseau sont installés sur le serveur V8.1.3, entrez la commande suivante afin de démarrer l'adaptateur de réseau spécifique qui est configuré avec l'adresse IP en cours de restauration sur ce serveur :

      ```
      ip link set dev ADAPTATEUR up
      ```

      Remplacez *ADAPTATEUR* dans la commande précédente par le nom de l'adaptateur indiqué à l'étape 3.a précédente afin de restaurer l'adresse IP d'origine du serveur V8.1.3 sur le serveur V8.1.3.

   L'adresse IP d'origine sur l'adaptateur de réseau V8.1.4 est maintenant restaurée. L'adaptateur de réseau V8.1.3 a également son adresse IP d'origine restaurée.

Résultats

Le serveur Cloud APM V8.1.4 devient le nouveau serveur actif.

Mise à niveau du serveur connecté à un serveur Db2 distant

Si le serveur Cloud APM V8.1.3 à partir duquel vous effectuez la mise à niveau est connecté à un serveur Db2 distant existant au lieu du serveur Db2 local par défaut, vous devez sauvegarder les bases de données séparément pour éviter tout problème entre le serveur V8.1.3 existant et le nouveau serveur V8.1.4 utilisant ces bases de données.

Avant de commencer

- Lorsque vous effectuez la mise à niveau du serveur Cloud APM, le serveur Db2 pour le serveur Cloud APM V8.1.4.0 doit être au même niveau de version que le serveur Db2 utilisé par le serveur Cloud APM V8.1.3. Vérifiez la version Db2 utilisée par le serveur Cloud APM V8.1.3 :
  - Si Db2 est installé sur le même système que le serveur Cloud APM, entrez la commande suivante pour vérifier la version de Db2 :

    ```
    rép_install/db2/V10.5/bin/db2level
    ```

    où *rép_install* est le répertoire où Db2 est installé.
  - Si Db2 est installé sur un système distant, demandez à l'administrateur Db2 de vérifier la version du serveur Db2.

  Important :

  Le serveur Db2 pour le serveur Cloud APM V8.1.4 doit être au même niveau de version que le serveur Cloud APM V8.1.3 au cours de la mise à niveau de ce dernier.

  Si la version Db2 de votre serveur Cloud APM V8.1.3 est Db2 Advanced Enterprise Server Edition V10.5 groupe de correctifs 9, suivez maintenant les étapes décrites dans la note technique Upgrading your Cloud APM server from V8.1.3 to V8.1.4 when your Db2 server is running V10.5 fix pack 9 pour continuer la mise à niveau du serveur Cloud APM de la version 8.1.3 vers la version 8.1.4.

  Si vous souhaitez utiliser Db2 V11.1 pour votre serveur Cloud APM V8.1.4, vous pouvez mettre à niveau votre serveur Db2 vers une version prise en charge de Db2 V11.1 une fois la mise à niveau du serveur Cloud APM terminée. Suivez la procédure décrite dans «Mise à niveau du serveur Db2 vers Db2 Advanced Workgroup Server Edition version 11.1.x», à la page 1089.
- Si votre serveur Cloud APM est connecté à un serveur Db2 distant, Db2 Advanced Workgroup Server Edition V11.1 est pris en charge lors de la mise à niveau de votre serveur Cloud APM de la version 8.1.3 à la version 8.1.4.
- Si vous mettez à niveau le serveur Cloud APM sur le même système et que vous disposez d'un serveur Db2 distant, suivez les instructions de la rubrique Mise à niveau du serveur sur le même système.
- Si votre serveur Cloud APM V8.1.3 est connecté à une base de données MongoDB distante, installez MongoDB V3.2.12. Pour plus d'informations, voir «Installation de MongoDB V3.2.12 sur votre système distant», à la page 942.
- AIX Le script backup.sh n'est pas pris en charge sous AIX. Utilisez les utilitaires Db2 pour sauvegarder vos bases de données. Pour plus d'informations, voir Backup overview et BACKUP DATABASE command dans l'ensemble de rubriques relatif à Db2 V10.5.0 disponible sur IBM Knowledge Center.
- AIX Le script restore.sh script n'est pas pris en charge sous AIX. Utilisez les utilitaires Db2 pour restaurer vos bases de données. Pour plus d'informations, voir RESTORE DATABASE command.
- Si LDAP est activé sur votre serveur Cloud APM V8.1.3 afin d'authentifier les utilisateurs de la console Cloud APM, suivez la procédure ci-dessous sur votre serveur Cloud APM V8.1.3 avant de sauvegarder les données V8.1.3 :

1. Récupérez la valeur de l'attribut *realm* dans le fichier `rép_install/wlp/usr/shared/config/ldapRegistry.xml`.
2. Vérifiez la valeur de l'attribut *oauthRealm* dans le fichier `rép_install/wlp/usr/shared/config/oauthVariables-onprem.xml`. Si la valeur de l'attribut *oauthRealm* ne correspond pas à la valeur de l'attribut *realm* dans le fichier `ldapRegistry.xml`, mettez à jour la valeur de l'attribut *oauthRealm* de sorte qu'elle corresponde à la valeur de l'attribut *realm*.
3. Suivez la procédure ci-dessous pour mettre à jour le fichier `rép_install/wlp/usr/servers/apmui/server-oauth2-tai.xml` afin d'ajouter l'utilisateur à partir du fichier `rép_install/wlp/usr/servers/server1/cscs/conf/cscsRoleAdmin.conf` :
   a. Recherchez la ligne de propriétés **<properties** et identifiez le paramètre **systemUser** ; s'il n'existe pas, vous devrez l'ajouter à l'étape suivante. Identifiez la balise fermante **/>** de la ligne de propriétés.
   b. Ajoutez une nouvelle ligne ou modifiez une ligne existante avant la balise fermante **/>**, comme suit :

      ```
      systemUser="testuser LDAP distinguished name"
      ```

      où *testuser* correspond à la chaîne user du fichier `cscsRoleAdmin.conf`, par exemple :

      ```
      systemUser="CN=testuser,CN=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
      ```

      Remarque : N'incluez pas le user:prefix ou le nom de domaine qui a été spécifié dans `cscsRoleAdmin.conf`.
   c. Confirmez que la balise fermante **/>** n'a pas été supprimée, puis sauvegardez et fermez le fichier.

- Si vous avez modifié le magasin de clés de confiance pour votre serveur Cloud APM V8.1.3, remplacez-le par le mot de passe par défaut avant de procéder à la mise à niveau du serveur. Une fois cette dernière terminée, vous pouvez rétablir votre mot de passe de magasin de clés de confiance personnalisé. Pour plus de détails, consultez cette procédure décrite dans Changing the password for the shared truststore.

Pourquoi et quand exécuter cette tâche

- Le serveur Cloud APM stocke les données dans les bases de données WAREHOUS, SCR32 et DATAMART sur le serveur Db2. Avant d'installer la V8.1.4 du serveur Cloud APM sur le système utilisé pour la mise à niveau, vous devez créer des copies de ces trois bases de données en leur attribuant des noms différents de ceux qui étaient utilisés pour le serveur V8.1.3.
- Dans cette procédure, les noms des trois bases de données Db2 sont désignés comme suit :

Tableau 201. Noms de base de données Db2

	Nom de la base de données V8.1.3	**Nouveau nom de la base de données V8.1.4**
Warehouse	WAREHOUS	W1
Datamart	DATAMART	D1
SCR	SCR32	S1

Des noms différents peuvent être utilisés pour les bases de données V8.1.4 ; il suffit de remplacer le nom indiqué dans le tableau 201 de la procédure suivante par le nom de votre choix.

- Dans la version 8.1.4, si votre serveur Cloud APM est connecté à un serveur Db2 distant qui s'exécute également sur un serveur Cloud APM V8.1.4, vous pouvez créer un nom personnalisé pour l'utilisateur d'instance Db2, ou vous pouvez accepter le nom par défaut `db2apm`. Dans les éditions précédentes de Cloud APM, seul le nom d'utilisateur d'instance `db2apm` était pris en charge. Pour la version V8.1.4, comme les étapes de cette procédure se rapportent à un serveur Db2 distant existant, c'est-à-dire un serveur Db2 distant pré-V8.1.4, vous devez effectuer ces étapes en tant qu'utilisateur `db2apm`.

- La plupart des étapes sont exécutées en tant que superutilisateur. D'autres sont exécutées en tant qu'utilisateur d'instance Db2 `db2apm`. Elles contiennent une commande **`su`** dans le nom d'utilisateur d'instance Db2 et un **`exit`** à la fin qui permet de revenir en mode superutilisateur.

Procédure

Pour cloner les bases de données WAREHOUS, SCR32 et DATAMART avant la mise à niveau et pour les sauvegarder séparément, effectuez les opérations suivantes en tant que superutilisateur.

1. Téléchargez l'image d'installation du serveur Cloud APM. Extrayez les fichiers d'installation du serveur correspondant à votre offre. Effectuez les étapes 1, à la page 957 à 4, à la page 957 dans «Mise à niveau du serveur côte à côte», à la page 955.
2. Copiez les scripts `backup.sh`, `rename.sh` et `restore.sh` à partir du répertoire `tools` et le script `setup-dbconfig-linux_64.bin` à partir du répertoire `packages/SCR` sur l'image d'installation du serveur Cloud APM V8.1.4 dans le système du serveur serveur Db2 distant. Vous pouvez vous connecter au serveur Db2 existant qui a été configuré pour Cloud APM V8.1.3.
3. Exécutez le script `backup.sh` sur le système du serveur Db2 distant. Si vous utilisez les ID et mot de passe de l'administrateur Cloud APM par défaut, exécutez `backup.sh` sans paramètre. Par exemple :

   ```
   [root]# /root/min/tools/backup.sh
   Exécution d'une sauvegarde...
   Traitement du composant "install"...
   Traitement du composant "db2"... Opération de sauvegarde terminée.
   Création du fichier de sauvegarde... Toutes les tâches se sont terminées avec succès.
   Votre sauvegarde est disponible dans le fichier suivant :
   /tmp/backups/backup_20160824_061708.tar
   ```

   Si vous utilisez les ID et mot de passe d'un utilisateur autre que celui par défaut, exécutez le script avec ces paramètres. Par exemple,

   ```
   [root]# /root/min/tools/backup.sh  -u nom_d'utilisateur -p mot_de_passe
    -z instance_db2_externe
   ```

   Où :

   nom_d'utilisateur
   ID utilisateur de l'administrateur Cloud APM autre que celui par défaut.

   mot_de_passe
   Mot de passe administrateur Cloud APM autre que celui par défaut.

   instance_db2_externe
   Nom de l'utilisateur d'instance serveur Db2 distante.

   Le nom du fichier de sauvegarde est indiqué dans la sortie.
4. Exécutez le script `setup_dbconfig-linux_64.bin` sur le système du serveur Db2 distant pour configurer la base de données SCR version 8.1.4. Exécutez le script en tant qu'utilisateur d'instance Db2 `db2apm` ayant exécuté le script pendant la création de la base de données SCR v8.1.2. N'exécutez pas le script en tant que superutilisateur.

   ```
   su - db2apm
   /path/setup-dbconfig-linux_64.bin -i console
   exit
   ```

   Suivez les invites de la console :

   a. A l'invite de sélection d'un environnement local, entrez 2 pour sélectionner l'anglais.
   b. Entrez 1 pour accepter le contrat de licence.
   c. Entrez le chemin d'accès absolu au dossier d'installation, ou appuyez sur la touche Entrée pour accepter le chemin par défaut. Le chemin par défaut est le chemin d'installation de `installation-dbconfig` pour la V8.1.3. Ne le modifiez pas, sauf s'il est incorrect. Dans cette procédure, le chemin d'accès est appelé `/opt/ibm/db2/tbsmdb`.

d. Entrez 1 pour sélectionner IBM Cloud Application Performance Management (APM) comme produit utilisant la base de données.

e. Entrez 1 pour sélectionner Simple comme type d'installation à exécuter.

f. Entrez 2 pour que le programme d'installation ne crée pas le schéma de base de données, notamment les tables, les espaces table et les vues.

g. Entrez les détails de configuration de la base de données suivants lorsque vous y êtes invité :

   Nom de la base de données (8 caractères au maximum) (VALEUR PAR DEFAUT : SCR32) : S1

   Nom d'hôte ou adresse IP de la base de données (VALEUR PAR DEFAUT) : *nom_hôte_ou_adresse_IP*

   Port de la base de données (VALEUR PAR DEFAUT : 50000) : *port*

   Chemin d'accès à la base de données (VALEUR PAR DEFAUT) : *chemin_par_défaut*

   Où :

   port Numéro de port qui a été spécifié lors de la création de la base de données SCR. Si vous ne connaissez pas la valeur, regardez le numéro de port spécifié pour le service db2c_db2apm dans le fichier /etc/services.

   chemin_par_défaut
   Système de fichiers où la base de données a été créée. Le chemin par défaut est le répertoire de base de l'utilisateur db2apm. Si un autre système de fichiers a été spécifié lors de la création de la base de données, indiquez-le.

h. Entrez 2 pour indiquer de ne pas chiffrer la base de données.

5. En tant que superutilisateur, exécutez le script restore.sh sur le système du serveur Db2 distant pour restaurer la sauvegarde que vous avez créée à l'étape 3, à la page 969. Ce fichier de sauvegarde est restauré avec les nouveaux noms des bases de données V8.1.4, W1, S1 et D1. Exécutez restore.sh avec les options et valeurs suivantes :

```
[root]# min/tools/restore.sh -f fichier_sauvegarde
-j nom_bd_mesure -k nom_bd_scr -l
nom_bd_datamart -z instance_db2_externe
```

   Par exemple :

```
[root]# min/tools/restore.sh -f /tmp/backups/backup_20150824_061708.tar
-j W1 -k S1 -l D1 -z db2apm
Restauration des données... Traitement du composant "db2"...
Opération de restauration terminée.
Toutes les tâches se sont terminées avec succès.
```

   Où :

   fichier_sauvegarde
   Fichier de sauvegarde que vous avez créé à l'étape 3, à la page 969.

   nom_bd_mesure
   Nouveau nom facultatif de la base de données de mesure.

   nom_bd_scr
   Nouveau nom facultatif de la base de données de topologie.

   nom_bd_datamart
   Nouveau nom facultatif de la base de données DATAMART.

   instance_db2_externe
   Nom de l'utilisateur d'instance serveur Db2 distante.

6. Mettez à niveau le schéma de base de données et les routines UDF Java dans la base de données SCR Db2. Entrez :

```
cd chemin_install/tbsmdb/tools/XMLtoolkit/bin
./scr_restore.sh -U db2apm -P passw0rd -n
```

où *chemin_install* correspond au chemin que vous avez entré lors de la configuration de `setup-dbconfig`.

Si vous ne voulez pas que le mot de passe apparaisse sur la ligne de commande, omettez l'indicateur `-P` ; le script vous demande alors le mot de passe. Par exemple :

```
./scr_restore.sh -n
Entrez le mot de passe de la base de données :
```

7. Entrez la commande suivante en tant qu'utilisateur `db2apm` pour chaque base de données afin d'ajuster le pool de mémoire tampon et le journal des transactions, après avoir déterminé la taille de votre environnement.

```
su - db2apm
db2 connect to W1
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size NBR_PAGES_W1
db2 disconnect W1
db2 connect to D1
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size NBR_PAGES_D1
db2 disconnect to D1
db2 connect to S1
db2 UPDATE DATABASE CONFIGURATION FOR S1 USING LOGSECOND 25
db2 alter bufferpool IBMDEFAULTBP IMMEDIATE size 5000
db2 alter bufferpool TBSMCFG16KBP IMMEDIATE size 1000
db2 alter bufferpool TBSM4KBP IMMEDIATE size 1000
db2 alter bufferpool TBSM32KBP IMMEDIATE size 1000
db2 alter bufferpool TBSMSCR16KBP IMMEDIATE size NBR_PAGES_S1
db2 disconnect to S1
exit
```

Où :

NBR_PAGES_W1
Nombre de pages de pool de mémoire tampon (pages de 8 K) : 50000 pour Petite ; 100000 pour Moyenne ou 200000 pour Grande.

NBR_PAGES_D1
Nombre de pages de pool de mémoire tampon (pages de 8 K) : 100000 pour Petite ; 200000 pour Moyenne ou 300000 pour Grande.

NBR_PAGES_S1
Nombre de pages de pool de mémoire tampon (pages de 16 K) : 30000 pour Petite ; 50000 pour Moyenne et 100000 pour Grande.

Estimez la taille de votre environnement (Petite, Moyenne ou Grande) d'après le tableau de la configuration requise pour le serveur dans «Configuration matérielle requise pour le serveur Cloud APM», à la page 92.

8. Installez IBM Data Server Client sur la machine virtuelle ou le système informatique que vous utilisez pour la mise à niveau vers le serveur Cloud APM V8.1.4 en effectuant l'étape 3 décrite dans la rubrique «Connexion à un serveur Db2 distant», à la page 129.
9. Installez la version 8.1.4 du serveur Cloud APM. Effectuez les étapes 5 à 13 de la rubrique «Mise à niveau du serveur côte à côte», à la page 955. Utilisez les informations des étapes 10 et 11 dans cette procédure afin de guider vos réponses.
10. Une fois que le script d'installation a détecté que la sauvegarde des informations du serveur Cloud APM V8.1.3 était configurée avec un serveur Db2 distant existant, répondez aux invites pour fournir ou accepter les valeurs par défaut des paramètres de configuration suivants afin d'établir une connexion avec la base de données Db2 distante :
    a. `Entrez le nom d'hôte/l'adresse IP de l'hôte DB ou acceptez la valeur par défaut [hôte_local] :`
    b. `Entrez le numéro de port d'instance DB2 ou acceptez la valeur par défaut [50000] :`
    c. `Entrez le mot de passe de l'utilisateur "itmuser" :`
    d. `Entrez le nom d'instance DB2 distante ou acceptez la valeur par défaut [db2apm] :`

e. `Entrez mot de passe de l'utilisateur d'instance "db2apm" :`

11. Lorsque vous êtes invité à entrer les noms des nouvelles bases de données V8.1.4 (W1, S1 et D1) que vous avez créées lorsque vous avez précédemment spécifié la commande **restore.sh**, acceptez les valeurs par défaut ou entrez de nouvelles valeurs selon vos besoins.

    Si vous prévoyez d'utiliser le serveur V8.1.3, entrez les noms des nouvelles bases de données (W1, S1 et D1) que vous avez créées lorsque vous avez exécuté la commande **restore.sh** à l'étape 5. Sinon, si vous acceptez les valeurs par défaut, vous endommagez les bases de données qui continuent d'être utilisées par la version 8.1.3 du serveur Cloud APM.

    Important : Si vous entrez les noms des nouvelles bases de données, ceux-ci doivent correspondre aux noms utilisés avec le script `restore.sh` à l'étape 5 sur le serveur Db2 distant :

    ```
    Entrez le nom de la base de données de mesure ou acceptez la valeur par défaut [WAREHOUS] : W1
    Entrez le nom de la base de données de topologie ou acceptez la valeur par défaut [SCR32] : S1
    Entrez le nom de la base de données de mesure ou acceptez la valeur par défaut [DATAMART] : D1
    ```

    L'installation du serveur Cloud APM V8.1.4 se poursuit.

    Si le programme d'installation détecte dans *rép_install*`/ccm/depot` des packages de configuration d'agent issus d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé les anciens packages et qu'il a créé les nouveaux packages d'agent. Les anciens packages sont nommés *rép_install*`/ccm/depot.old`.

    Si le programme d'installation détecte dans *rép_install* un répertoire `keyfiles` issu d'une installation précédente du serveur Cloud APM, il vous avertit qu'il a renommé l'ancien répertoire `keyfiles` et qu'il en a créé un nouveau. L'ancien répertoire `keyfiles` est nommé *rép_install*`/keyfiles.old`.L'analyse des prérequis de votre environnement commence et prend un moment. Une fois l'installation terminée, la version 8.1.4 du serveur Cloud APM est configurée avec le serveur Db2 distant existant, qui est la même instance que la version 8.1.3 mais qui utilise des bases de données différentes. Les bases de données utilisées sont celles créées à l'étape 5.

12. Si vous ne continuez pas à utiliser le serveur Cloud APM V8.1.3, vous pouvez utiliser les bases de données par défaut V8.1.3 sur votre système V8.1.4 en effectuant les étapes suivantes :

    a. Une fois l'installation de la version 8.1.4 terminée, arrêtez les systèmes serveur Cloud APM V8.1.3 et V8.1.4 en entrant la commande suivante à partir de n'importe quel répertoire sur l'un des deux systèmes :

       ```
       apm stop_all
       ```

    b. Sur le système serveur Db2 distant, exécutez le script `rename.sh`. Indiquez les noms des bases de données que vous avez créées à l'étape 5 en tant qu'arguments.

       Par exemple, la commande suivante renomme les bases de données V8.1.4 W1 en WAREHOUS, S1 en SCR32 et D1 en DATAMART :

       ```
       ./rename.sh W1 S1 D1
       ```

    c. Sur le système du serveur Cloud APM version 8.1.4, démarrez les composants kafka et server1 en entrant les commandes suivantes :

       ```
       apm start kafka
       apm start server1
       ```

    d. Sur le système V8.1.4 mis à niveau, entrez la commande suivante :

       rép_install`/ccm/db_common.sh restore_original_db_names`

       où *rép_install* désigne le répertoire d'installation du serveur Cloud APM.

    Le serveur Cloud APM V8.1.4 est reconfiguré pour utiliser les bases de données d'origine : WAREHOUS, SCR32 et DATAMART.

13. Arrêtez le système serveur Cloud APM V8.1.3, s'il fonctionne, en entrant la commande suivante à partir de n'importe quel répertoire :

    ```
    shutdown -P now
    ```

14. Réaffectez l'adresse IP ou l'adresse IP et le nom d'hôte du serveur Cloud APM V8.1.3 au serveur V8.1.4. La réaffectation de l'adresse IP seulement ou de l'adresse IP combinée au nom d'hôte est liée à votre configuration.

- Si vous utilisez l'adresse IP du serveur Cloud APM pour connecter vos agents à votre serveur, effectuez les étapes décrites dans la rubrique Réaffectation de l'adresse IP du serveur à un autre serveur.
- Si vous utilisez le nom d'hôte du serveur Cloud APM pour connecter vos agents à votre serveur, effectuez les étapes décrites dans la rubrique Réaffectation de l'adresse IP et du nom d'hôte du serveur à un autre serveur.

15. Migrez la configuration de la Passerelle hybride :
    - Pour migrer la Passerelle hybride immédiatement après une restauration, exécutez ces commandes sur le serveur Cloud APM en tant que superutilisateur :
      a. Copiez le fichier `config.properties` restauré dans le répertoire `ccm` :

         ```
         cp rép_install/ccm/properties/config.properties.restored rép_install/ccm/properties/
         config.properties
         ```

      b. Mettez à jour les date et heure du fichier `config.properties` afin de recharger la configuration de toutes les passerelles hybrides déjà en cours d'exécution :

         ```
         touch config.properties
         ```

      c. Copiez le fichier `config.properties` mis à jour dans le composant Central Configuration Services :

         ```
         cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
         CentralConfigurationServer.war/common/config.properties
         ```

    - Si des configurations ont été effectuées au niveau du système mis à niveau après la restauration, procédez comme suit :
      a. Copiez ces deux lignes à partir du fichier *rép_install*`/ccm/properties/config.properties.restored` :

         ```
         com.ibm.tivoli.ccm.encryption\:key=
         com.ibm.tivoli.ccm.gaian.connect\:gaianReq=
         ```

      b. Remplacez les mêmes lignes dans *rép_install*`/ccm/properties/config.properties` par celles que vous venez de copier.
      c. Copiez `config.properties` dans le composant Central Configuration Services :

         ```
         cp rép_install/ccm/properties/config.properties rép_install/wlp/usr/servers/min/dropins/
         CentralConfigurationServer.war/common/config.properties
         ```

    Pour vous assurer que le fichier `config.properties` sous *rép_install*`/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/common/` a bien été remplacé, vérifiez que les date et heure modifiées correspondent aux date et heure en cours.

Résultats

La mise à niveau du serveur Cloud APM vers la V8.1.4 est terminée et le serveur est connecté au serveur Db2 distant que vous utilisiez avec la V8.1.3.

Que faire ensuite

- Si vous utilisez les certificats prêts à l'emploi par défaut pour accéder à la console Cloud APM, vous devez suivre les étapes dans cette note technique V8.1.4 Application Performance Management UI certificates are expiring in upgraded environments pour mettre à jour les certificats par défaut afin qu'ils n'expirent pas en avril 2019.
- Avant d'utiliser laconsole Cloud APM, que vous avez mise à niveau, effacez le cache de votre navigateur Web et redémarrez le navigateur. Effacer le cache évite les problèmes que les nouvelles fonctions de cette mise à jour ont créé dans certaines des interfaces utilisateur.
- Si vous souhaitez utiliser les anciens packages de configuration d'agent issus d'une précédente installation pour effectuer les installations d'agent, effectuez les étapes suivantes :
  1. Accédez au répertoire *rép_install*`/ccm`.
  2. Supprimez le fichier `agentconfig`.

3. Remplacez le nom du fichier `agentconfig.old` par `agentconfig`.

- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3, vous devez redéfinir clientAuthentication sur true. Copiez l'élément xml ssl qui contient l'attribut enabledCiphers du fichier *rép_install*`/wlp/usr/servers/min/server.xml` vers le fichier *rép_install*`/wlp/usr/servers/min/user-exit.xml` s'il n'existe pas déjà dans le fichier `user-exit.xml`. Ajoutez ensuite la ligne `clientAuthentication="true"` après la ligne enabledCiphers dans le fichier `user-exit.xml`. Supprimez l'élément XML ssl du fichier `server.xml`. L'exemple de code ci-dessous indique où ajouter la ligne `clientAuthentication="true"` dans le fichier `user-exit.xml`.

  ```
  <ssl
  id="defaultSSLConfig"
  sslProtocol="TLSv1.2"
  enabledCiphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
  clientAuthentication="true"
  serverKeyAlias="server_key"
  clientKeyAlias="IBM_Tivoli_Monitoring_Certificate"
  keyStoreRef="defaultKeyStore"/>
  ```

- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3 et que vous avez utilisé les certificats par défaut, redéfinissez le protocole de communication utilisé par les agents du serveur Cloud APM sur HTTPS. Pour obtenir des instructions, voir Configuration du protocole de communications pour les agents de serveur.
- Si vous avez configuré la communication HTTPS entre le serveur Cloud APM et les agents dans votre serveur Cloud APM V8.1.3 et que vous n'avez pas utilisé les certificats par défaut, procédez comme suit :
  1. Codez le mot de passe du magasin de clés du serveur (xor) que vous avez utilisé lors de la création des certificats pour le serveur Cloud APM V8.1.3 :

     ```
     /opt/ibm/wlp/bin/securityUtility encode
     ```

  2. Copiez l'élément xml keyStore du fichier *rép_install*`/ibm/wlp/usr/servers/min/server.xml` dans le fichier *rép_install*`/wlp/usr/servers/min/user-exit.xml` s'il n'existe pas déjà dans le fichier `user-exit.xml`. Dans le fichier `user-exit.xml`, remplacez ensuite la valeur de l'attribut password par le mot de passe que vous venez de coder à l'étape 1. Supprimez l'élément XML keyStore du fichier `server.xml`.
  3. Accédez au répertoire *rép_install*.
  4. Supprimez le répertoire `keyfiles`.
  5. Remplacez le nom du fichier `keyfiles.old` par `keyfiles`.
  6. Mettez à jour les certificats utilisés par les agents de surveillance pour se connecter au serveur Cloud APM afin qu'ils exploitent le nouveau magasin de clés. Pour plus d'informations, voir «Configuration des certificats entre le serveur et les agents», à la page 222.
  7. Mettez à jour le protocole de communication et les certificats utilisés par les agents du serveur Cloud APM. Pour obtenir des instructions, voir Configuration du protocole de communications pour les agents de serveur.
- Si le système où vous avez installé le serveur Cloud APM utilise LDAP pour authentifier le superutilisateur ou les utilisateurs Db2 et que vous avez mis à jour les mots de passe de l'utilisateur `itmuser` et des utilisateurs d'instance Db2 à l'étape 6, exécutez l'étape 10 dans «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138.
- Contrôlez les paramètres de la base de données WAREHOUS qui ont été appliqués par le processus de restauration.

  ```
  update database config for warehous using DFT_DEGREE any
  update database config for warehous using LOGBUFSZ 1024
  update database config for warehous using LOCKLIST AUTOMATIC
  update database config for warehous using SORTHEAP AUTOMATIC
  update database config for warehous using SHEAPTHRES_SHR AUTOMATIC
  update database config for warehous using NUM_IOCLEANERS AUTOMATIC
  update database config for warehous using NUM_IOSERVERS AUTOMATIC
  update database config for warehous using LOGFILSIZ 4096
  update database config for warehous using LOGPRIMARY 10
  ```

```
update database config for warehous using DBHEAP AUTOMATIC
update database config for warehous using LOGSECOND 40
update database config for warehous using AVG_APPLS AUTOMATIC
update database config for warehous using logarchmeth1 OFF
update database config for warehous using logarchmeth2 OFF
update database config for warehous using DATABASE_MEMORY 250000 AUTOMATIC
```

Cloud APM ne prend pas en charge l'élagage des journaux de base de données. Aussi, les paramètres `logarchmeth1` et `logarchmeth2` sont définis sur `OFF`. Si vous sauvegardez la base de données d'entrepôt et que votre environnement prend en charge l'élagage des journaux, modifiez ces paramètres.

- La plupart des agents Cloud APM V8.1.3 sont compatibles avec le serveur Cloud APM V8.1.4. Après avoir mis à niveau ce dernier vers la version 8.1.4.0, vous devez cependant mettre à niveau les agents suivants :
  - Si vous utilisez l'agent Synthetic Playback, vous devez le mettre à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence. Vous devez ensuite appliquer le dernier correctif temporaire du serveur Cloud APM 8.1.4.0, disponible depuis Fix Central.
  - Monitoring Agent for WebSphere Applications doit être mis à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence.
  - Monitoring Agent for MongoDB doit être mis à niveau à l'aide du dernier package d'agent dans Passport Advantage. Pour afficher les numéros de référence Passport Advantage pour les packages d'agent, voir : Numéros de référence.

Mise à niveau de vos agents

De nouveaux fichiers archive contenant des agents de surveillance mis à niveau sont régulièrement disponibles pour téléchargement. Les fichiers archive sont disponibles à partir de IBM Passport Advantage.

Avant de commencer

Pour les agents suivants, une tâche spécifique à l'agent doit être exécutée avant de suivre la procédure de mise à niveau :

- Pour les agents sous AIX, si vous êtes connecté en tant qu'utilisateur non superutilisateur, vous devez supprimer l'une des bibliothèques de la mémoire avant de lancer la procédure d'installation pour mettre à niveau l'agent. Suivez les instructions décrites dans «Agents sous AIX : arrêt de l'agent et exécution de **slibclean** avant la mise à niveau», à la page 978.
- Pour l'agent HMC Base sous AIX, si vous le mettez à niveau en tant qu'utilisateur non superutilisateur, vous devez d'abord arrêter l'agent HMC Base et effacer les bibliothèques dépendantes du cache. Suivez les instructions de la rubrique «agent HMC Base sous AIX : Arrêt de l'agent en tant qu'utilisateur non superutilisateur et exécution de **slibclean** avant la mise à niveau», à la page 979
- Pour l'agent Microsoft .NET, vous devez supprimer le collecteur de données de vos applications .NET avant de mettre à niveau l'agent. Suivez les instructions décrites dans «agent Microsoft .NET : suppression du collecteur de données .NET avant la mise à niveau», à la page 980.
- Pour l'Agent Node.js, supprimez les plug-in de collecteur de données des applications Node.js avant de le mettre à niveau. Suivez les instructions décrites dans «Agent Node.js : suppression des plug-in de collecteur de données avant la mise à niveau», à la page 979.
- Pour l'Agent Ruby, vous devez supprimer le collecteur de données de vos applications Ruby avant de mettre à niveau l'agent. Suivez les instructions décrites dans «Agent Ruby : suppression des plug-in de collecteur de données avant la mise à niveau», à la page 981.
- Pour l'agent HTTP Server, vous devez arrêter le serveur HTTP avant de mettre à niveau l'agent.
- Pour l'Agent WebSphere MQ, si vous avez activé le suivi des transactions pour l'agent dans la version antérieure, vous devez arrêter l'instance d'agent avant de mettre à niveau l'agent.

- Pour l'Agent SAP NetWeaver Java Stack, lors d'une mise à niveau de la version V8.1.3.2 vers la version V8.1.4, vous devez arrêter toutes les instances SAP NetWeaver Java Stack configurées avec le collecteur de données avant de mettre à niveau l'agent.
- Pour l'Agent Skype for Business Server, si vous effectuez une mise à niveau d'une ancienne version vers la version 8.1.4.0.2 côté agent, le nom de l'agent est modifié en Skype for Business Server. De plus, après avoir mis à niveau le support via SDA, vous devez redémarrer le service APMUI de sorte à répercuter le nouveau nom de l'agent (Skype for Business Server) côté MIN Server ; dans le cas contraire, l'ancien nom de l'agent (MS Lync Server) s'affichera sur le tableau de bord MIN Server.
- Pour Agent Tomcat, si vous souhaitez mettre à niveau TEMA Core Framework sous Windows, vous devez arrêter l'agent et le serveur. Suivez les instructions de la rubrique Agent Tomcat : mise à niveau de TEMA Core Framework sous Windows

Pourquoi et quand exécuter cette tâche

Si une nouvelle version de l'agent est disponible, l'exécution du script d'installation met automatiquement l'agent à niveau. Si aucune version plus récente de l'agent n'est disponible, un message s'affiche pour indiquer que l'agent est déjà installé ; l'agent installé n'est pas affecté.

Pour installer un agent mis à niveau, procédez comme suit :

Procédure

- «Installation des agents sur les systèmes AIX», à la page 165
- «Installation des agents sur les systèmes Linux», à la page 170
- «Installation des agents sur les systèmes Windows», à la page 177

Résultats

L'agent est mis à niveau vers la version la plus récente. Si aucune version plus récente de l'agent de surveillance n'est disponible, un message s'affiche pour indiquer que l'agent est déjà installé ; l'agent installé n'est pas affecté.

Que faire ensuite

Après une mise à niveau d'un agent Windows, redémarrez celui-ci s'il n'est pas automatiquement configuré et démarré par le programme d'installation de Windows. Exécutez la commande suivante pour vérifier le statut de l'agent :

```
./nom-agent.bat status
```

Utilisez l'une des méthodes suivantes pour démarrer l'agent :

- Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**. Cliquez avec le bouton droit de la souris sur un agent et cliquez sur **Start**.
- Exécutez la commande suivante :

  ```
  ./nom-agent.bat start
  ```

Pour plus d'informations sur les commandes relatives à l'agent de surveillance, y compris le nom à utiliser, le contrôle du statut, etc., voir «Utilisation des commandes de l'agent», à la page 213. Pour plus d'informations sur les agents démarrés automatiquement et manuellement, voir Chapitre 8, «Déploiement d'agents et de collecteurs de données», à la page 155.

- Pour l'agent Hadoop, procédez comme suit après la mise à niveau de l'agent basé sur un socket (version 8.1.2, groupe de correctifs 2 ou antérieure) vers l'agent basé sur une API REST (version 8.1.3 ou ultérieure) :
  1. Pour éviter la génération de journaux inutiles, supprimez le code de 17 lignes dans les fichiers `hadoop-metrics2.properties` de tous les noeuds Hadoop.
  2. Arrêtez les services Hadoop.

3. Supprimez de tous les noeuds du cluster Hadoop le fichier `Plugin.jar` qui a été copié par le programme d'installation d'agent.
4. Démarrez les services Hadoop.

Pour plus d'informations sur le code de 17 lignes et le fichier `Plugin.jar`, voir Configuration de noeuds Hadoop.

- Pour l'agent HMC Base, après l'avoir mis à niveau de la version 6.2.2.6 à la version 6.2.2.7, vous devez de nouveau le configurer et le redémarrer. Pour plus d'informations, voir «Configuration de la surveillance de HMC Base», à la page 314.
- Pour l'agent HTTP Server, si vous mettez à niveau l'agent à partir d'une version antérieure à 1.0.0.4 vers 1.0.0.4 ou ultérieure, vous devez également mettre à jour le fichier `.conf`, utilisé par le serveur HTTP, pour remplacer le fichier de configuration du collecteur de données précédent par le fichier qui vient d'être généré. Vous devez également ajouter la nouvelle instance d'agent à la console. Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 319.
- Pour l'agent Microsoft .NET, après l'avoir mis à niveau, configurez le collecteur de données. Pour plus d'informations, voir «Enregistrement du collecteur de données», à la page 485.

  Si vous avez installé l'agent dans un nouveau répertoire, vous devez modifier le chemin du répertoire Bin du service Profiler à l'aide de la commande service controller (`sc`). Par exemple,

  ```
  sc \\localhost config DotNetProfilerService binPath=
  "${rép_install}\qe\bin\DotNetProfilerService.exe
  ```

  où *rép_install* correspond au nouveau répertoire d'installation.
- Pour l'Agent Node.js, après l'avoir mis à niveau, configurez les collecteurs de données d'agent. Pour obtenir des instructions, voir «Configuration de l'Agent Node.js», à la page 549.
- Pour l'Agent OpenStack, si vous souhaitez le configurer pour utiliser OpenStack Identity API v3, reconfigurez toutes les instances d'agent et mettez à jour le fichier de configuration du collecteur de données d'agent. Pour obtenir des instructions, voir «Agent OpenStack : reconfiguration des instances de l'agent pour utiliser OpenStack Identity API v3», à la page 981.
- Pour l'Agent Ruby, après l'avoir mis à niveau, configurez le collecteur de données. Pour plus d'informations, voir «Configuration du collecteur de données de diagnostic», à la page 672.
- Pour l'Agent WebSphere Applications, après l'avoir mis à niveau, migrez le collecteur de données en exécutant la commande *base_cd*`/bin/migrate.sh/bat` à partir du répertoire d'installation de la nouvelle version de l'agent et redémarrez l'instance de serveur d'applications. Pour plus d'informations, voir «Agent WebSphere Applications : migration du collecteur de données», à la page 982.
- Linux Si vous souhaitez mettre à niveau une ancienne version de l'agent installée dans le répertoire `/opt/ibm/ccm/agent`, procédez comme suit sur le système Linux :
  1. Si vous confirmez vouloir migrer la configuration de l'agent de l'ancien répertoire d'installation `/opt/ibm/ccm/agent` vers le nouveau répertoire d'installation (par exemple, `/opt/ibm/apm/agent`), vous devez démarrer l'agent dans le nouvel emplacement d'installation.

     Restriction : L'ancienne version de l'agent est arrêtée automatiquement dans l'ancien emplacement d'installation, mais elle n'est pas démarrée automatiquement dans le nouvel emplacement d'installation.
  2. Une fois que vous avez vérifié que l'agent fonctionne dans le nouveau répertoire d'installation, vous devez désinstaller l'ancienne version de l'agent du répertoire `/opt/ibm/ccm/agent`. Si vous souhaitez supprimer tous les agents, exécutez la commande **`/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all`**.

Conservation des changements apportés à la configuration des agents

Les utilisateurs avancés peuvent appliquer des valeurs de substitution à la personnalisation des composants. L'application de valeurs de substitution permet de conserver les valeurs lors d'une mise à niveau.

Avant de les appliquer d'une manière globale, testez les changements apportés à votre environnement.

Pourquoi et quand exécuter cette tâche

- Ces instructions s'appliquent aux agents Linux et AIX. Pour obtenir la liste des codes produit et des commandes utilisées pour arrêter et démarrer les agents, voir «Utilisation des commandes de l'agent», à la page 213.
- Le processus de l'agent Windows conserve les changements de configuration par conception : les variables mises à jour dans le fichier k*cp*cma.ini, où *cp* correspond au code produit, sont conservées dans la section Override Local Settings. Elles sont utilisées lors de chaque configuration pour mettre à jour les entrées du registre Windows que les agents utilisent au moment de l'exécution.
- Les paramètres personnalisés dans les fichiers *.cp*.environment et .global.environment sont perdus après la mise à niveau de l'agent. Pour conserver vos paramètres, effectuez les modifications de personnalisation dans les fichiers *cp*.environment et global.environment. Les paramètres de ces fichiers ne sont pas écrasés par une mise à niveau de l'agent.

Procédure

Pour sauvegarder les changements de configuration apportés au fichier d'environnement et les conserver après la mise à niveau de l'agent, procédez comme suit :

1. Créez et mettez à jour l'un des fichiers suivants, où *rép_install* est le répertoire d'installation de l'agent (par exemple, le répertoire Linux par défaut /opt/ibm/apm/agent/ ou le répertoire AIX par défaut /opt/ibm/ccm/agent/) :

Nom du fichier	Description
***rép_install*/config/*cp*.environment**	Le terme *cp* dans le nom de fichier désigne le code produit de l'agent, par exemple mq ou rz.
***rép_install*/config/global.environment**	Mettez à jour le fichier d'environnement global de manière à appliquer les changements devant affecter tous les types d'agent.

   Par exemple, as.environment est le fichier d'environnement persistant de l'Agent WebSphere Applications. .as.environment est remplacé lorsque l'agent est mis à niveau vers une nouvelle version. Définissez les variables au format *clé=valeur*, où *clé* est le nom de la variable d'environnement et *valeur* est la valeur ou le paramètre (tel que **KDC_FAMILIES=${KDC_FAMILIES}HTTP:10001**).
2. Une fois que vous avez mis à jour les paramètres de variable, enregistrez et fermez le fichier d'environnement, puis redémarrez les agents concernés.

Résultats

Les mises à jour sont appliquées à tous les agents de même type ou, si vous avez mis à jour le fichier d'environnement global, à tous les agents relevant du serveur Cloud APM. Les changements sont conservés malgré les mises à niveau des versions de l'agent.

Agents sous AIX : arrêt de l'agent et exécution de `slibclean` avant la mise à niveau

Si vous mettez à niveau un agent en tant qu'utilisateur non superutilisateur sur les systèmes AIX, vous devez effectuer cette tâche. Avant d'exécuter le programme d'installation de l'agent, vous devez arrêter l'agent et exécuter la commande **slibclean** pour nettoyer la bibliothèque libkududp.a.

Procédure

1. Arrêtez l'agent en exécutant l'une des commandes suivantes, dans le cas où l'agent prendrait en charge plusieurs instances ou non :
   - ./*nom*-agent.sh stop
   - ./*nom*-agent.sh stop *nom_instance*

Voir «Utilisation des commandes de l'agent», à la page 213.

2. Exécutez la commande suivante avec les privilèges de superutilisateur.
   slibclean

   Voir slibclean Command dans le composant IBM Knowledge Center.

Résultats

L'agent est arrêté et la bibliothèque `libkududp.a` est nettoyée.

Que faire ensuite

Exécutez le programme d'installation pour mettre à niveau l'agent vers la version que vous avez téléchargée. Voir Chapitre 9, «Installation des agents», à la page 161. Si la mise à niveau échoue, réamorcez le serveur et répétez la procédure.

agent HMC Base sous AIX : Arrêt de l'agent en tant qu'utilisateur non superutilisateur et exécution de `slibclean` avant la mise à niveau

Avant de mettre à niveau l'agent HMC Base en tant qu'utilisateur non superutilisateur sur AIX, vous devez l'arrêter et exécuter **slibclean** pour effacer les bibliothèques dépendantes du cache.

Pourquoi et quand exécuter cette tâche

Procédure

1. Exécutez la commande suivante en tant qu'utilisateur non superutilisateur pour arrêter l'agent.
   `hmc_base-agent.sh stop`
2. Exécutez la commande suivante avec les privilèges de superutilisateur.
   slibclean

   Voir slibclean Command dans le composant IBM Knowledge Center.

Résultats

L'agent HMC Base est arrêté et les bibliothèques dépendantes sont effacées.

Que faire ensuite

Exécutez le programme d'installation d'agent pour mettre à niveau l'agent HMC Base.

Agent Node.js : suppression des plug-in de collecteur de données avant la mise à niveau

Avant de mettre à niveau l'Agent Node.js, supprimez les plug-in de surveillance de votre application Node.js.

Pourquoi et quand exécuter cette tâche

En fonction de la version de votre Agent Node.js, vous devez suivre une procédure spécifique pour supprimer les plug-ins de surveillance de votre application Node.js. Pour connaître la version de l'agent, voir Commande de version d'agent.

Procédure

1. Supprimez les plug-in de collecteur de données au début du fichier d'application Node.js :

- Si vous mettez à niveau l'Agent Node.js à partir de la version 01.00.12.00 vers la version 01.00.13.00, procédez comme suit :
  - Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js :

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
    ```

    où *KNJ_NPM_LIB_LOCATION* correspond au répertoire du dossier `lib` de votre répertoire d'installation global du package npm. Le répertoire par défaut est `/usr/local/lib`.
  - Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js :

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
    ```
  - Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js :

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
    ```
- Si vous mettez à niveau l'Agent Node.js à partir de la version 01.00.10.00 vers la version 01.00.13.00, procédez comme suit :
  - Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js.

    ```
    require('rép_install/lx8266/nj/bin/plugin/knj_index.js');
    ```

    , où *rép_install* correspond au répertoire d'installation de l'Agent Node.js.
  - Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js.

    ```
    require('rép_install/lx8266/nj/bin/plugin/knj_deepdive.js');
    ```
  - Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js .

    ```
    require('rép_install/lx8266/nj/bin/plugin/knj_methodtrace.js');
    ```

2. Redémarrez l'application Node.js pour désactiver les plug-ins de collecteur de données.
   - Si la version actuelle de l'Agent Node.js est01.00.10.00, les plug-ins du collecteur de données sont supprimés dès maintenant.
   - Si la version de votre Agent Node.js actuel est la version 01.00.12.00, passez à l'étape suivante.
3. Exécutez la commande `./uninstall.sh` à partir du répertoire *rép_install*`/lx8266/nj/bin` pour supprimer les paramètres d'agent précédents.

Que faire ensuite

Mettez à niveau l'Agent Node.js. Voir «Mise à niveau de vos agents», à la page 975.

Agent Response Time Monitoring : mise à niveau de module IBM HTTP Server Response Time

Si vous surveillez IBM HTTP Server à l'aide du module IBM HTTP Server Response Time ou de l'agent HTTP Server, procédez comme suit pour mettre à niveau votre installation.

agent Microsoft .NET : suppression du collecteur de données .NET avant la mise à niveau

Avant de mettre à niveau l'agent Microsoft .NET, supprimez le collecteur de données .NET de vos applications .NET.

Procédure

1. Désenregistrez tous les modules du collecteur de données. En tant qu'administrateur, entrez :
   ```
   cd rép_install\qe\bin configdc unregisterdc all
   ```
   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Redémarrez les applications .NET.

Que faire ensuite

Mettez à niveau l'agent Microsoft .NET. Voir «Mise à niveau de vos agents», à la page 975.

Agent OpenStack : reconfiguration des instances de l'agent pour utiliser OpenStack Identity API v3

Pour mettre à niveau l'Agent OpenStack afin d'utiliser OpenStack Identity API v3, vous devez, après avoir installé la dernière version de l'agent, reconfigurer toutes les instances de l'agent et mettre à jour le fichier de configuration du collecteur de données.

Pourquoi et quand exécuter cette tâche

Cette tâche est requise uniquement si vous mettez à niveau l'agent pour utiliser OpenStack Identity API v3.

Procédure

1. Reconfigurez toutes les instances de l'agent existantes. Pour des instructions détaillées, voir «Configuration de l'Agent OpenStack», à la page 568.
2. Recherchez le fichier de configuration `ksg_dc_nom_instance.cfg` du collecteur de données d'agent, où *nom_instance* correspond au nom que vous avez spécifié pour l'instance d'agent. Si le fichier n'existe pas, copiez *rép_install*`/lx8266/sg/bin/ksg_dc.cfg` dans le répertoire *rép_install*`/config` et renommez le fichier `ksg_dc_nom_instance.cfg`. Par exemple, si le nom de l'instance est `OS1`, changez le nom en `ksg_dc_OS1.cfg`.
3. Ajoutez la section suivante au fichier `ksg_dc_nom_instance.cfg` :
   ```
   #OpenStack authentication information
   [OS_authentication_info]
   OS_project_domain_name=Default
   OS_user_domain_name=Default
   OS_cert_path=
   ```
4. Redémarrez l'instance d'agent en exécutant les commandes suivantes :
   ```
   rép_install/bin/openstack-agent.sh stop nom_instance
   rép_install/bin/openstack-agent.sh start nom_instance
   ```
   , où *nom_instance* correspond au nom de l'instance d'agent à configurer.

Agent Ruby : suppression des plug-in de collecteur de données avant la mise à niveau

Avant de mettre à niveau l'Agent Ruby, supprimez les plug-in de surveillance de votre application Ruby.

Procédure

1. Supprimez le collecteur de données de l'ancienne version en lançant la commande suivante :
   ```
   gem uninstall stacktracer
   ```
2. Accédez au répertoire principal de votre application, ouvrez son `Gemfile` et supprimez la ligne suivante : `gem 'stacktracer', 'version'`
   Où *version* correspond au numéro de version de l'Agent Ruby.

3. Dans le répertoire principal de votre application, entrez : `bundle install`

Que faire ensuite

Mettez à niveau l'Agent Ruby. Voir «Mise à niveau de vos agents», à la page 975.

Agent WebSphere Applications : migration du collecteur de données

Après avoir mis à jour l'agent, vous devez migrer le collecteur de données de manière interactive ou en mode silencieux.

Migration du collecteur de données en mode interactif

Vous pouvez migrer un niveau de maintenance antérieur du collecteur de données en mode interactif à l'aide de l'utilitaire de migration.

Avant de commencer

Linux AIX Si vous avez installé WebSphere Application Server ou WebSphere Portal Server à l'aide d'un compte utilisateur non superutilisateur, avant d'exécuter les utilitaires de configuration, vérifiez que l'utilisateur non superutilisateur dispose des privilèges de lecture et écriture sur les répertoires d'agent suivants dans *rép_install*`/yndchome/7.3.0.14.06`, *rép_install* représentant le répertoire d'installation de l'Agent WebSphere Applications :

- `data`
- `bin`
- `runtime`
- `logs`

Le cas échéant, utilisez la commande `chmod 777` pour attribuer les droits en lecture et écriture. En outre, connectez-vous à l'aide du même ID utilisateur qui a servi pour installer le serveur d'applications.

Pourquoi et quand exécuter cette tâche

Vous pouvez migrer un niveau de maintenance antérieur du collecteur de données en mode interactif à l'aide de l'utilitaire de migration. Si vous souhaitez migrer un grand nombre d'instances de serveur d'applications, il peut être plus pratique d'utiliser l'utilitaire de migration en mode silencieux.

Important :

- Vous pouvez uniquement migrer les niveaux de maintenance antérieurs à la version 7.3 du collecteur de données. La version du collecteur de données est indiquée dans le répertoire de base du collecteur de données.
- Il n'est pas possible de migrer les niveaux de maintenance de la version 7.3 vers la version 7.3, groupe de correctifs 1. Vous devez annuler la configuration du collecteur de données et désinstaller la version d'agent 7.3, puis installer la version d'agent 7.3, groupe de correctifs 1 et configurer à nouveau le collecteur de données.

Procédure

1. Linux AIX Connectez-vous sous le nom de l'utilisateur utilisé pour installer le serveur d'applications.
2. Démarrez l'utilitaire de migration à partir du répertoire d'installation de la dernière version de l'agent.

   Linux AIX Lancez la commande *base_cd*`/bin/migrate.sh`

   Windows Exécutez la commande *base_cd*`\bin\migrate.bat`

3. L'utilitaire affiche les adresses IP de toutes les cartes réseau qui sont trouvées sur le système informatique local. Entrez le nombre qui correspond à l'adresse IP à utiliser.
4. L'utilitaire recherche et répertorie tous les serveurs configurés par niveau de maintenance antérieur de collecteur de données. Les collecteurs de données sont regroupés par niveau de maintenance. Sélectionnez une ou plusieurs instances de serveur d'applications dans la liste.

   La liste peut comporter les instances de serveur WebSphere et Liberty traditionnelles. Les instances de serveur WebSphere traditionnelles peuvent figurer sous différents profils.

   Conseil :
   - Si plusieurs instances d'un profil sont surveillées, vous devez toutes les sélectionner afin de les migrer simultanément.
   - Migrez tous les serveurs figurant sous le profil Liberty en même temps. Une migration partielle des serveurs configurés pourrait provoquer des problèmes de stabilité.

   A faire :
   - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter.
   - Dans un environnement de déploiement réseau, l'agent de noeud et le gestionnaire de déploiement doivent s'exécuter.
   - Il n'est pas nécessaire d'exécuter les serveurs Liberty au cours de la migration.
5. Entrez le numéro correspondant à l'instance de serveur d'applications dont le collecteur de données est en train de migrer ou entrez un astérisque (*) pour faire migrer le collecteur de données de toutes les instances de serveur d'applications.

   Pour spécifier un sous-ensemble de serveurs, entrez les numéros des serveurs en les séparant par une virgule. Par exemple : `1,2,3`.

   L'utilitaire de migration intègre automatiquement chaque collecteur de données à l'agent de surveillance. Les valeurs d'hôte et de port de l'agent de surveillance sont récupérées dans les fichiers de configuration existants.
6. Entrez un alias pour chaque serveur sélectionné. La valeur par défaut correspond à l'alias de serveur existant.
7. Pour l'instance de serveur Liberty, entrez le répertoire de base de la JVM lorsque vous y êtes invité. Par exemple, `/opt/IBM/java`.
8. L'utilitaire détermine si WebSphere Global Security est activé pour chacun des profils dans lesquels la collecte de données est migrée. Si WebSphere Global Security est activé pour un ou plusieurs profils, indiquez s'il faut récupérer les paramètres de sécurité dans le fichier de propriétés d'un client : Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP (Simple Object Access Protocol). Si la sécurité globale est activée pour un profil, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à IBM WebSphere Application Server la console d'administration pour le profil.

   Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client Application Server avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI et le fichier `soap.client.props` pour une connexion SOA.
9. Entrez 1 pour permettre à l'utilitaire d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié et passez à l'étape 11, à la page 984. Sinon, entrez 2 pour saisir le nom d'utilisateur et le mot de passe.

   Important : La connexion à la console d'administration WebSphere Application Server peut prendre du temps.
10. Indiquez le nom d'utilisateur et le mot de passe pour chaque profil où WebSphere Global Security est activé.

11. L'utilitaire migre la collecte de données pour chaque instance de serveur d'applications sélectionnée. Il affiche un message d'état indiquant si la migration de chaque serveur s'est effectuée correctement.
12. Redémarrez les instances comme indiqué par l'utilitaire. La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré.

Résultats

Le collecteur de données est migré au dernier niveau de maintenance installé.

Que faire ensuite

L'utilitaire de migration conserve les paramètres configurés dans la version antérieure du collecteur de données. Pour modifier ces paramètres, vous pouvez exécuter l'utilitaire de configuration ou de reconfiguration en mode interactif ou silencieux à partir du répertoire *base_cd*\bin du nouveau collecteur de données. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.

Migration du collecteur de données en mode silencieux

Vous pouvez migrer un niveau de maintenance antérieur du collecteur de données en mode silencieux à l'aide de l'utilitaire de migration.

Avant de commencer

Linux AIX Si vous avez installé WebSphere Application Server ou WebSphere Portal Server à l'aide d'un compte utilisateur non superutilisateur, avant d'exécuter les utilitaires de configuration, vérifiez que l'utilisateur non superutilisateur dispose des privilèges de lecture et écriture sur les répertoires d'agent suivants dans *rép_install*/yndchome/7.3.0.14.06, *rép_install* représentant le répertoire d'installation de l'Agent WebSphere Applications :

- data
- bin
- runtime
- logs

Le cas échéant, utilisez la commande chmod 777 pour attribuer les droits en lecture et écriture. En outre, connectez-vous à l'aide du même ID utilisateur qui a servi pour installer le serveur d'applications.

Pourquoi et quand exécuter cette tâche

Un exemple de fichier de propriétés silencieux, sample_silent_migrate.txt, est fourni avec l'utilitaire de migration. Ce fichier se trouve dans le répertoire *rép_install*/yndchome/7.3.0.14.06/bin.

Lorsque vous créez votre fichier de propriétés silencieux, tenez compte des remarques suivantes :

- Dans le fichier, une ligne commençant par un signe dièse (#) est considérée comme un commentaire, et n'est pas traitée. Si le signe dièse est utilisé ailleurs dans la ligne, on ne le considère pas comme le début d'un commentaire. Vous pouvez donc utiliser le caractère dièse dans les mots de passe ou à d'autres fins.
- Chaque propriété est décrite sur une ligne distincte, au format suivant : propriété = valeur.

  propriété
  Le nom de la propriété. La liste de propriétés valides que vous pouvez configurer est affichée dans le tableau 202, à la page 985. Ne modifiez pas ou ne supprimez pas les propriétés du fichier d'échantillon qui ne sont pas mentionnées dans la table.

  valeur La valeur de la propriété. Des valeurs par défaut pour certaines propriétés sont déjà fournies. Vous pouvez supprimer des valeurs par défaut pour laisser des valeurs de propriété en blanc. Une valeur vide est traitée comme si la propriété n'était pas indiquée, par opposition à

l'utilisation de la valeur par défaut. Si vous voulez utiliser des valeurs par défaut, vous pouvez mettre en commentaire la propriété dans le fichier.

- Les mots de passe sont en texte en clair.
- Les propriétés et leurs valeurs distinguent les majuscules et minuscules.

Le tableau 202 décrit les propriétés disponibles lors de la migration du collecteur de données en mode silencieux.

Tableau 202. Propriétés disponibles pour l'exécution de l'utilitaire de migration en mode silencieux

Propriété	**Commentaire**
migrate.type	Doit avoir pour valeur `AD`.
default.hostip	Si le système informatique utilise plusieurs adresses IP, indiquez l'adresse IP que le collecteur de données doit utiliser.
itcam.migrate.home	Indique le répertoire de base du collecteur de données correspondant à la version de maintenance antérieure du collecteur de données. Le répertoire n'est pas supprimé au cours de la migration.
was.wsadmin.connection.host	Indique le nom de l'hôte auquel l'outil wsadmin se connecte. Dans un environnement Network Deployment, spécifiez la connexion wsadmin au gestionnaire de déploiement. Dans un environnement autonome, indiquez la connexion wsadmin au serveur.
was.wsadmin.username	Spécifie l'ID utilisateur d'un utilisateur autorisé à se connecter à la console d'administration d'IBM WebSphere Application Server. Cet utilisateur doit posséder le rôle d'agent sur le serveur d'applications.
was.wsadmin.password	Indique le mot de passe qui correspond à l'utilisateur indiqué dans la propriété `was.wsadmin.username`.
was.appserver.profile.name	Indique le nom du profil de serveur d'applications à configurer. **A faire :** Cette propriété n'est pas requise pour le profil Liberty.
was.appserver.home	Indique le répertoire de base de WebSphere Application Server.
was.appserver.cell.name	Indique le nom de cellule de WebSphere Application Server. **A faire :** Cette propriété n'est pas requise pour le profil Liberty.
was.appserver.node.name	Indique le nom de noeud de WebSphere Application Server. **A faire :** Cette propriété n'est pas requise pour le profil Liberty.
was.appserver.server.name	Spécifie l'instance de serveur d'applications figurant dans le profil de serveur d'applications devant être migrée vers la nouvelle version du collecteur de données. Le fichier de propriétés silencieux peut comporter plusieurs occurrences de cette propriété.

Important :

- Vous pouvez uniquement migrer les niveaux de maintenance antérieurs à la version 7.3 du collecteur de données. La version du collecteur de données est indiquée dans le répertoire de base du collecteur de données.

- Il n'est pas possible de migrer les niveaux de maintenance de la version 7.3 vers la version 7.3, groupe de correctifs 1. Vous devez annuler la configuration du collecteur de données et désinstaller la version d'agent 7.3, puis installer la version d'agent 7.3, groupe de correctifs 1 et configurer à nouveau le collecteur de données.

Procédure

1. Spécifiez les options de configuration dans le fichier de propriétés de migration en mode silencieux.
2. Lancez la commande de démarrage de l'utilitaire de migration en mode silencieux à partir du répertoire d'installation de la dernière version de l'agent.
   - Linux AIX *base_cd*/bin/migrate.sh -silent *sample_silent_migration_filename*
   - Windows *base_cd*\bin\migrate.bat -silent *sample_silent_migration_filename*

Résultats

Le collecteur de données est migré au dernier niveau de maintenance installé.

Que faire ensuite

L'utilitaire de migration conserve les paramètres configurés dans la version antérieure du collecteur de données. Pour modifier ces paramètres, vous pouvez exécuter l'utilitaire de configuration ou de reconfiguration en mode interactif ou silencieux à partir du répertoire *dc_home*\bin du nouveau collecteur de données. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 773.

Agent Tomcat : mise à niveau de TEMA Core Framework sous Windows

Pour mettre à niveau TEMA Core Framework sous Windows pour l'Agent Tomcat, vous devez arrêter l'agent et le serveur pour que la mise à jour de l'infrastructure TEMA aboutisse.

Procédure

1. Préparez la configuration du serveur Tomcat.
2. Installez et configurez l'agent Tomcat.
3. Connectez-vous au tableau de bord IBM Cloud Application Performance Management, accédez à **Configuration d'agent** > **Tomcat**, sélectionnez une instance de l'Agent Tomcat et cliquez sur **Enable TT/DD**.
4. Redémarrez le serveur Tomcat.
5. Pour appliquer IBM APM CORE FRAMEWORK, arrêtez l'agent et le serveur Tomcat.
6. Accédez à TEMA/<IBM APM CORE FRAMEWORK_HOME>. Exécutez la commande **apmpatch.bat <répertoire d'installation de l'agent Tomcat>**.
   L'infrastructure est mise à niveau.
7. Vérifiez la version IBM APM CORE FRAMEWORK mise à niveau en exécutant les instructions ci-après.
   Goto <répertoire d'installation de l'agent Tomcat>\InstallITM
   Run: KinCInfo.exe -i.
8. Démarrez le serveur et l'agent Tomcat.

Mise à niveau de vos collecteurs de données

De nouveaux fichiers archive contenant des collecteurs de données mis à niveau sont régulièrement disponibles pour téléchargement. Les fichiers archive sont disponibles à partir de IBM Passport Advantage.

Avant de commencer

Si vous mettez à niveau votre serveur Cloud APM, vous devez également mettre à niveau vos collecteurs de données.

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau un collecteur de données, procédez comme suit :

Procédure

- Annulez la configuration du collecteur de données à partir de vos applications locales et/ou IBM Cloud :
  - Pour le collecteur de données J2SE, les étapes d'annulation de la configuration ne sont pas requises.
  - Pour le collecteur de données Liberty, suivez les instructions dans «Annulation de la configuration du collecteur de données pour les applications IBM Cloud», à la page 851 et/ou «Annulation de la configuration du collecteur de données pour les applications sur site», à la page 844.
  - Pour le collecteur de données Node.js, suivez les instructions dans «Annulation de la configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 561 et/ou «Annulation de la configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 567.
  - Pour le collecteur de données Python, suivez les instructions dans «Annulation de la configuration du collecteur de données Python pour les applications IBM Cloud», à la page 628 et/ou «Annulation de la configuration du collecteur de données Python pour les applications sur site», à la page 634.
  - Pour le collecteur de données Ruby, suivez les instructions dans «Annulation de la configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 680.
- Téléchargez le module du collecteur de données.
- Reconfigurez le collecteur de données pour surveiller vos applications locales et/ou IBM Cloud :
  - Pour le collecteur de données Node.js, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir les instructions, voir «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 555 et/ou «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 561.
  - Pour le collecteur de données Python, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir les instructions, voir «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 624 et/ou «Configuration du collecteur de données Python pour les applications sur site», à la page 629.
  - Pour le collecteur de données Liberty, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir les instructions, voir «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 845 et/ou «Configuration du collecteur de données Liberty pour les applications sur site», à la page 813.
  - Pour le collecteur de données J2SE, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir des instructions, voir «Configuration de la surveillance de J2SE», à la page 418.
  - Pour le collecteur de données Ruby, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir des instructions, voir «Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 677.

Résultats

Le collecteur de données est mis à niveau vers la version la plus récente.

Chapitre 13. Gestion

L'administration de l'infrastructure Cloud APM et des agents se compose de tâches de maintenance telles que la modification des mots de passe et la personnalisation des tâches telles que l'ajout et la modification des applications.

Démarrage de la console Cloud APM

Connectez-vous à la console Cloud APM depuis votre navigateur afin de consulter l'état de vos applications dans les tableaux de bord.

Avant de commencer

- L'adresse URL de connexion est l'adresse IP du serveur Cloud APM.
- Pour être sûr que l'interface utilisateur ne soit pas tronquée, utilisez une résolution minimale de 1280 x 1024.
- Pour des performances optimales, utilisez l'un des navigateurs pris en charge. Pour une liste des navigateurs pris en charge, accédez à la page System requirements (APM Developer Center). Sélectionnez l'un des liens du produit IBM Cloud Application Performance Management et cliquez sur le lien «Serveur». Dans le rapport qui s'affiche, cliquez sur «Navigateurs Web» ou faites défiler l'écran jusqu'à cette option.

Procédure

1. Ouvrez une fenêtre de navigateur et entrez l'adresse URL suivante, où *hôte_serveur* correspond à l'adresse IP du serveur :

   `https://hôte_serveur:9443`

   Vous pouvez également entrer `http://hôte_serveur:8080`, bien que l'adresse URL soit automatiquement remplacée par le https sécurisé et le numéro de port `9443`.
2. Lorsque vous êtes invité à indiquer votre ID de connexion, entrez les données d'identification suivantes pour l'utilisateur par défaut ou entrez les données d'identification qui ont été affectées à votre administrateur :
   - **Nom d'utilisateur** *apmadmin*
   - **Mot de passe** *apmpass*

   Les données d'identification utilisateur initiales après l'installation du serveur Cloud APM sont `apmadmin` avec le mot de passe `apmpass`.

Résultats

Une fois que vous vous êtes connecté, la page Mise en route s'affiche avec des options d'apprentissage pour **Tâches de l'utilisateur** et **Tâches de l'administrateur** et permet d'accéder à **Ressources communautaires**.

Que faire ensuite

- Familiarisez-vous avec les éléments de l'interface utilisateur en cliquant sur le lien hypertexte pour effectuer une visite du tableau de bord Cloud APM. Regardez les vidéos des tâches d'utilisateur et des tâches d'administrateur pour vous aider à démarrer le système en utilisant et en personnalisant votre environnement Cloud APM.
- Ajoutez des applications pour afficher les tableaux de bord de vos ressources suivant des regroupements logiques, tels que Commande en ligne. Pour obtenir des instructions, voir «Gestion des applications», à la page 1145.

© Copyright IBM Corp. 2015, 2018

- Créez des seuils pour le test des conditions qui, lorsqu'ils sont atteints, ouvrent un événement. Par exemple, un seuil peut ouvrir un événement lorsque l'espace de stockage est utilisé à 90 %. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1002.
- Ajoutez et affectez des utilisateurs à des groupes d'utilisateurs et des rôles pour contrôler l'accès aux ressources gérées et aux fonctions de la console Cloud APM. Pour plus d'informations, voir «Gestion des accès utilisateur», à la page 1020.
- Pour plus d'informations sur la surveillance de la Liste d'applications Java IBM et la Pile d'intégration IBM, voir Chapitre 5, «Scénarios», à la page 97.
- Si, au lieu de la page de mise en route ou du Tableau de bord d'Application Performance, votre navigateur accède au site Web d'IBM, votre identificateur utilisateur n'a aucun droit sur la console Cloud APM. Vous devez demander l'accès à votre administrateur.
- Si aucun indicateur n'apparaît pour une source de données, consultez le forum Cloud Application Performance Management sur developerWorks. Recherchez le terme «tableau de bord» dans le forum, répondez à une entrée pour poser une question associée ou créez une entrée et décrivez le symptôme.
- Si vous démarrez la console Cloud APM depuis Internet Explorer 8, 9 ou 10 et que vous obtenez une erreur signalant que `la page ne peut pas s'afficher`, vous devrez peut-être activer l'option de sécurité, TLS 1.2. Pour plus d'informations, recherchez «tls» sur le forum forum Cloud Application Performance Management.

Seuils et groupes de ressources

Les seuils déterminent certaines conditions, telles que le nombre de transactions par minute inférieur à 100 et ouvrent un événement quand les conditions ont été remplies. Utilisez des seuils pour surveiller les problèmes réels et éventuels sur vos ressources surveillées. Affectez des seuils aux groupes de ressources pour la surveillance sur tous les systèmes gérés du même type qui appartiennent au groupe.

Informations de référence

Examinez les informations de référence pour en savoir plus sur les seuils, les seuils prédéfinis pour les agents, les groupes de ressources auxquels ils sont affectés et la personnalisation des seuils.

Seuils prédéfinis

Vos agents de surveillance sont fournis avec des *seuils prédéfinis* activés et démarrés avec l'agent. La première fois que vous ouvrez le Gestionnaire de seuils, après avoir installé l'agent, la liste de seuils qui s'affiche pour le type de source de données sélectionné correspond aux seuils prédéfinis. Ces seuils prédéfinis sont affectés au groupe de ressources système par défaut de l'agent et indiqués dans la colonne **Groupes affectés**.

Si vous modifiez un seuil prédéfini, que ce soit pour changer le nom ou la condition, le seuil n'est plus considéré comme un seuil prédéfini mais comme un *seuil personnalisé*. Cependant, vous pouvez redéfinir le groupe de ressources affecté pour un seuil prédéfini du groupe de systèmes par défaut sur un groupe défini par l'utilisateur et il reste un seuil prédéfini.

Si vous préférez ne pas utiliser les seuils prédéfinis, vous pouvez les désactiver dans la page Configuration avancée (voir «Activation des seuils», à la page 1121). La désactivation des seuils prédéfinis n'a pas pour effet de les supprimer du gestionnaire de seuils ; elle supprime uniquement leur affectation de groupe et les rend ainsi inactifs. Après avoir désactivé les seuils prédéfinis, vous pouvez ouvrir le gestionnaire de seuils et vous rendre compte que la colonne **Groupes affectés** est vide pour chaque seuil prédéfini (voir «Exemples de seuils désactivés», à la page 992).

Vous pouvez activer le seuil comme seuil personnalisé en l'affectant à n'importe quel groupe de ressources disponible.

Seuils personnalisés

Les nouveaux seuils que vous créez sont les seuils personnalisés, comme indiqué dans la colonne **Origine** du gestionnaire de seuils. Si vous modifiez un seuil prédéfini, ce devient également un seuil personnalisé et son origine passe de «Prédéfini» à «Personnalisé».

Exécution d'une commande

Une fois qu'un événement a été ouvert pour un seuil défini sur true, vous pouvez exécuter automatiquement une commande ou un script de commandes sur le système surveillé pour lequel l'événement a été ouvert. Vous pouvez par exemple vouloir consigner des informations, déclencher un bip audible ou arrêter un travail qui consomme trop ressources.

La commande respecte la syntaxe suivante :

```
&{jeu_données.attribut}
```

où *jeu_données* est le nom du jeu de données et *attribut* est le nom d'attribut tel qu'affiché dans l'éditeur de seuil. Si le jeu de données ou le nom d'attribut contient un espace, remplacez l'espace par un trait de soulignement.

L'exemple suivant montre comment transmettre le paramètre de nom de disque à une ressource gérée :

```
/scripts/clean_logs.sh &{disque_KLZ.nom_disque}
```

Vous pouvez transférer un ou plusieurs attributs depuis le jeu de données. S'ils sont spécifiés, les attributs multiples sont transférés dans la commande dans l'ordre ($1, $2, etc.).

La commande s'exécute à partir de la ligne de commande avec le même compte utilisateur que celui avec lequel l'agent ou le collecteur d'agent a démarré. Par exemple, si l'agent s'exécute en tant que superutilisateur, le superutilisateur exécute la commande sur le système géré.

Les options suivantes contrôlent la fréquence d'exécution de la commande :

Sélectionnez ☐ **Lors du premier événement uniquement** si l'ensemble de données renvoie plusieurs lignes et que vous souhaitez n'exécuter la commande que pour la première occurrence de l'événement dans l'échantillon de données. Désélectionnez cette case pour exécuter la commande pour chaque ligne qui génère un événement.

Sélectionnez ☐ **Pour chaque intervalle vrai consécutif** pour exécuter la commande chaque fois que le seuil est défini sur true. Désélectionnez cette case pour exécuter la commande lorsque le seuil a la valeur true, mais pas une deuxième fois tant que le seuil n'a pas la valeur false, suivi par une autre évaluation true dans un intervalle ultérieur.

Groupes de ressources

Les groupes de ressources représentent une collection de systèmes gérés et déterminent comment les seuils sont répartis. Vous affectez un seuil au groupe de ressources qui inclut les systèmes gérés où il doit s'exécuter.

Tous les seuils prédéfinis ont une affectation de groupe de ressources par défaut, qui est le groupe défini par le système pour le type d'agent, tel que Db2 et Microsoft IIS.

Vous pouvez créer des groupes de ressources personnalisées et sélectionner les systèmes gérés à inclure dans chaque groupe. Vous pouvez avoir plusieurs types d'agent dans un groupe de ressources personnalisées ; les seuils affectés au groupe sont distribués uniquement aux systèmes gérés du même type d'agent. Par exemple, un seuil qui est créé avec des attributs de système d'exploitation Linux OS affecté à un groupe de ressources de systèmes gérés Linux OS, MongoDB et Python est distribué aux systèmes gérés Linux OS.

Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 995.

Statut des événements dans le Tableau de bord d'Application Performance

Les gravités de statut affichées dans le Tableau de bord d'Application Performance indiquent la gravité d'événement la plus élevée pour l'application, le groupe, le sous-groupe et l'instance de système géré sélectionnés.

Après avoir sélectionné une application depuis le navigateur ou une zone récapitulative dans le tableau de bord **Toutes mes applications**, un tableau de bord à onglets présente les différentes

facettes de votre application. L'onglet Evénements fournit des informations sur les événements pour l'élément de navigateur sélectionné, comme décrit dans «Statut de l'événement», à la page 1156.

Les modifications de seuil affectent également les autres seuils associés au même agent de surveillance

Après la création, la modification ou la suppression d'une définition de seuil, ou la modification de la liste des seuils qui sont distribués sur un agent de surveillance, tous les événements échantillonnés sont fermés pour les agents sur lesquels le seuil a été distribué. Après la fermeture des événements, les agents de surveillance rouvrent les événements dès lors qu'une condition de seuil est évaluée à true. Sur la console Cloud APM, les événements fermés disparaissent de la console jusqu'à ce qu'ils soient rouverts avec une nouvelle valeur d'**horodatage**. Si vous recevez les notifications d'événement par courrier électronique, vous recevrez les notifications des événements ouverts et fermés par ce biais.

Imaginez, par exemple, que vous disposez d'un groupe de ressources personnalisées intitulé Systèmes de site, auquel vous affectez des seuils et des agents de système d'exploitation Linux et WebSphere Applications. Vous créez un nouveau seuil de système d'exploitation Linux et l'affectez à Systèmes de site. Tous les événements échantillonnés ouverts sur les agents de système d'exploitation Linux qui sont affectés à Systèmes de sites sont fermés. Ensuite, les événements échantillonnés sont rouverts si les conditions de seuil sont encore à true.

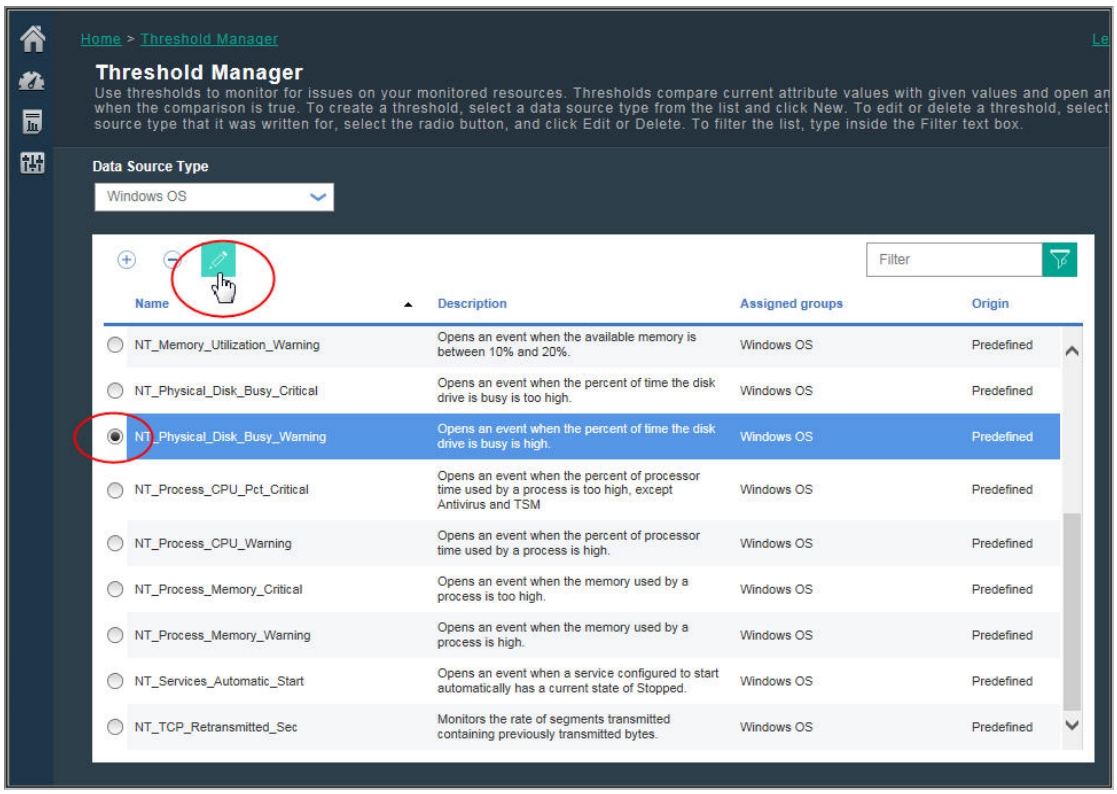
Exemples de seuils désactivés

Vous pouvez désactiver les seuils prédéfinis pour tous les agents dans votre environnement. Vous pouvez également désactiver des seuils séparément, qu'ils soient prédéfinis ou personnalisés. Lorsqu'un seuil est désactivé, il ne s'exécute pas sur les systèmes gérés et aucun événement n'est ouvert.

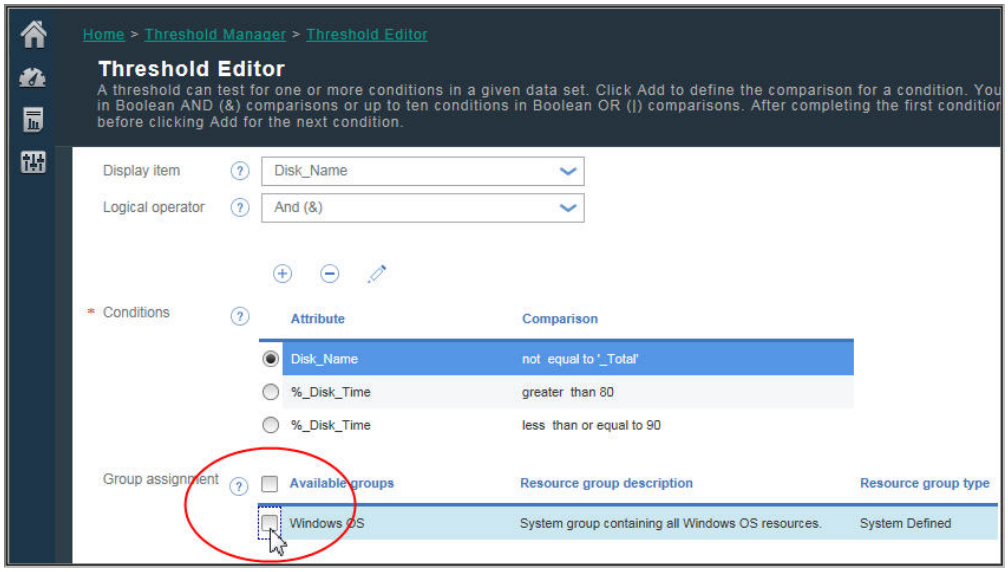
Pour désactiver un seuil, supprimez ses affectations de groupe de ressources. Un paramètre de Configuration avancée est également disponible pour désactiver tous les seuils prédéfinis pour tous les agents.

Désactivation d'un seuil unique

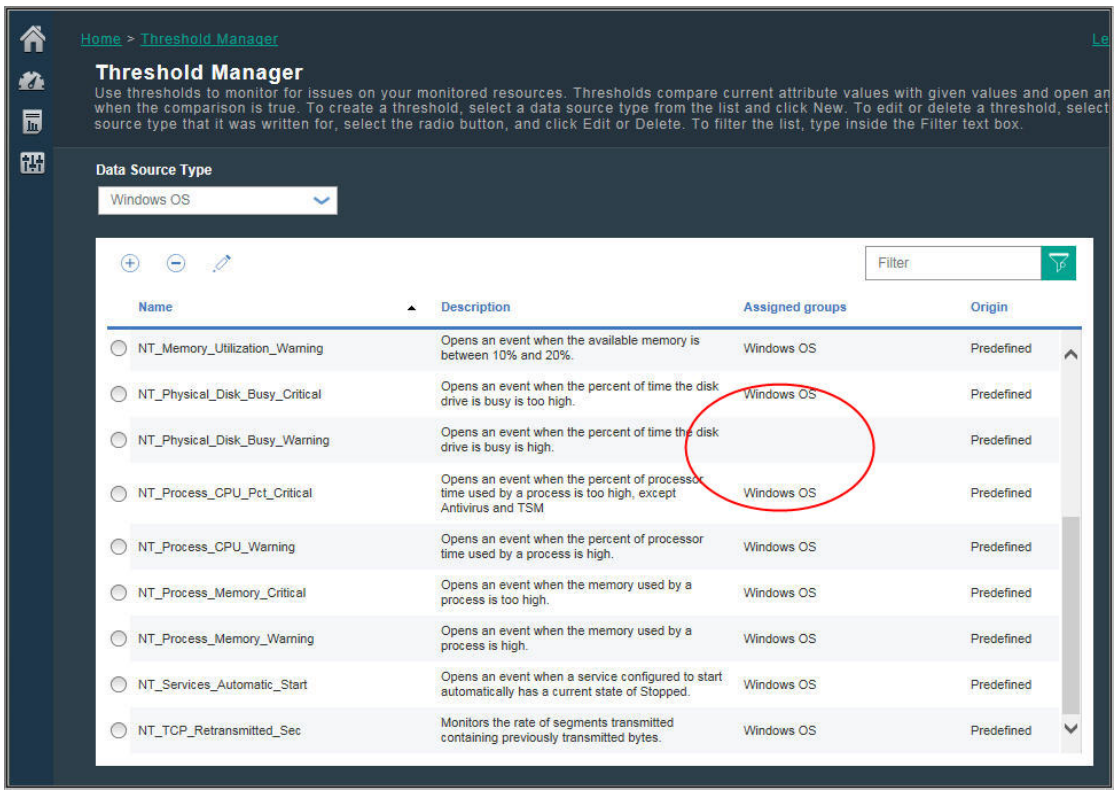
Dans cette image, le seuil à désactiver est sélectionné dans le Gestionnaire de seuils et l'utilisateur clique sur Editer :



Le seuil est ouvert dans l'éditeur de seuil. L'utilisateur désélectionne la case du groupe de ressources affecté dans la zone **Affectation de groupes** :

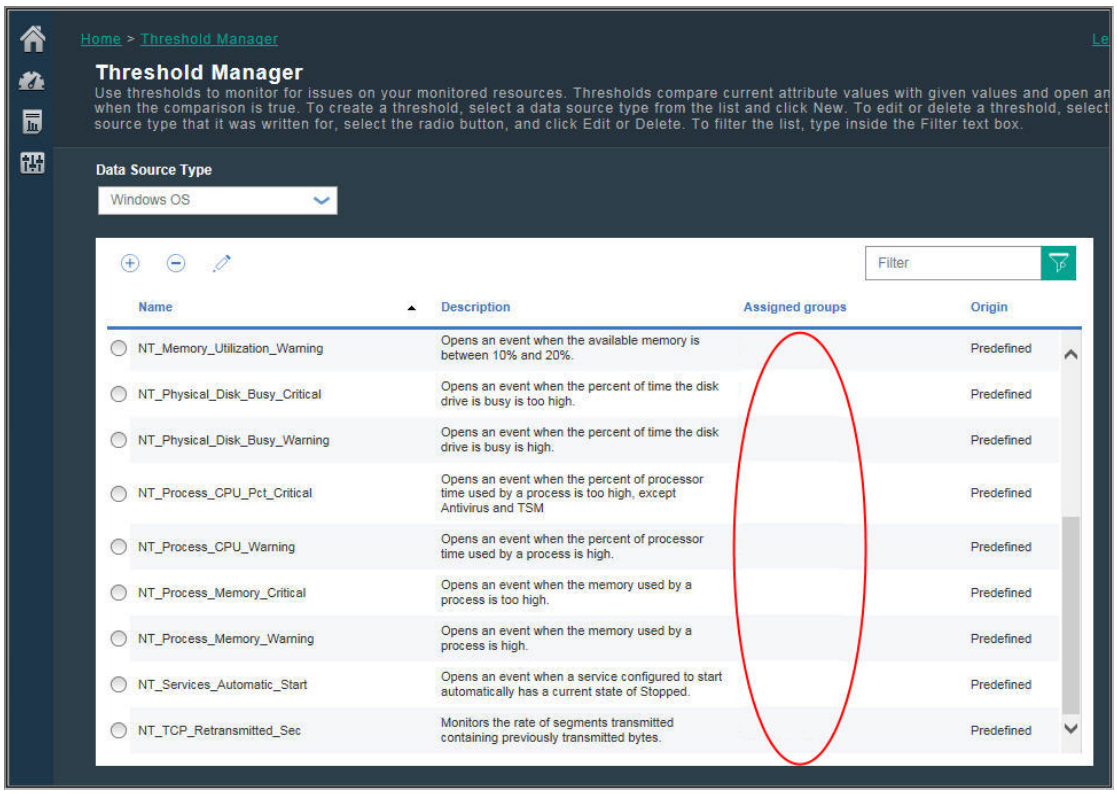


Une fois que l'utilisateur a cliqué sur **Sauvegarder**, le gestionnaire de seuil est affiché. Le seuil est désactivé, et la colonne Groupes affectés est vide :



Désactivation de tous les seuils prédéfinis

Désactivez tous les seuils prédéfinis pour tous les agents de surveillance sur la page Configuration avancée, comme décrit dans «Activation des seuils», à la page 1121. Lorsque vous ouvrez ensuite le gestionnaire de seuil, la colonne Groupes affectés est vide pour chaque seuil prédéfini, indiquant que les seuils sont inactifs :



Concepts associés:

«Informations de référence», à la page 990
Examinez les informations de référence pour en savoir plus sur les seuils, les seuils prédéfinis pour les agents, les groupes de ressources auxquels ils sont affectés et la personnalisation des seuils.

Référence associée:

«Gestionnaire de seuils», à la page 1002
Le Gestionnaire de seuils permet de consulter les seuils prédéfinis d'un agent de surveillance et de créer et d'éditer des seuils.

Gestionnaire de groupes de ressources

Votre environnement surveillé peut comporter plusieurs systèmes gérés pouvant être catégorisés par objectif. Ces systèmes possèdent souvent les mêmes exigences de seuil. Utilisez le gestionnaire de groupes de ressources pour organiser les systèmes gérés en groupes auxquels vous pouvez affecter des seuils. Vous pouvez également créer des groupes de ressources correspondant à vos stratégies de contrôle d'accès basé sur les rôles.

Une fois que vous avez cliqué sur **Configuration du système** > **Gestionnaire de groupes de ressources**, la page est affichée avec une table des groupes de ressources définis. Dans un premier temps, un groupe de systèmes prédéfini s'affiche pour chaque type d'agent de surveillance installé, comme `Windows OS`. Chaque groupe de systèmes contient tous les seuils prédéfinis de l'agent.

Votre accès au gestionnaire de groupes de ressources et aux groupes de ressources est contrôlé par vos droits d'utilisateur. Pour pouvoir afficher un groupe de ressources, vous devez disposer des droits d'affichage correspondants ; de la même manière, pour pouvoir créer, modifier ou supprimer un groupe de ressources, vous devez disposer de droits de modification.

Cette table contient des outils permettant de gérer les groupes de ressources.

- **Nouveau** ouvre l'Editeur de groupe de ressources pour affecter des systèmes gérés et des seuils.

- Sélectionnez un groupe de ressources pour afficher les ressources affectées et les seuils affectés au groupe dans la sous-fenêtre adjacente.
- Sélectionnez un groupe de ressources et cliquez sur **Editer** afin d'ouvrir l'Editeur de groupe de ressources pour modifier les affectations de système géré et de seuil.
- Sélectionnez un groupe de ressources dont vous ne voulez plus et cliquez sur **Supprimer**. Après confirmation de la suppression, les seuils qui étaient affectés au groupe doivent être affectés à un autre groupe si vous voulez qu'ils continuent à s'exécuter sur vos systèmes gérés.
- Vous pouvez cliquer dans la zone de texte du filtre et entrer la valeur du filtre. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour Arrière.

Le tableau contient les groupes de ressources disponibles :

Nom du groupe de ressources
Les groupes prédéfinis sont nommés en fonction de leur type d'agent ; les groupes personnalisés sont nommés par l'auteur.

Description du groupe de ressources
Un groupe prédéfini est décrit comme étant un *groupe de systèmes* pour la ressource surveillée ; les groupes personnalisés sont décrits par l'auteur.

Un groupe de systèmes, tel que `Linux OS`, inclut tous les seuils prédéfinis pour l'agent et tous les systèmes gérés sur lesquels l'agent est installé. Vous pouvez éditer un groupe de systèmes pour affecter ou supprimer des seuils, mais vous ne pouvez pas affecter ou supprimer des systèmes gérés. Les systèmes gérés sont affectés automatiquement à un groupe de systèmes du même type, y compris ceux issus de votre domaine Tivoli Monitoring si une Passerelle hybride est configurée.

Certains groupes de ressources système ont un lien avec les agents qui prennent en charge les sous-noeuds. En fonction du type d'agent, les sous-noeuds et/ou le noeud agent peuvent être ajoutés aux applications. Si seuls les sous-noeuds peuvent être ajoutés aux applications définies, vous ne pouvez pas visualiser les événements associés aux seuils qui ont été définis pour le noeud agent. Toutefois, les événements peuvent être transférés à un gestionnaire d'événements tel que Netcool/OMNIbus. De même, les abonnés IBM Cloud Application Performance Management peuvent configurer Alert Notification.

Type du groupe de ressources
Les groupes prédéfinis sont *définis par le système*. Un groupe prédéfini est associé à chaque type d'agent que vous avez installé dans votre environnement.

Les groupes personnalisés que vous, ou tout autre utilisateur, créez dans votre environnement sont *définis par l'utilisateur*.

Editeur de groupe de ressources

Une fois que vous avez cliqué sur **Nouveau** pour ajouter un groupe ou après avoir sélectionné un groupe et cliqué sur **Editer** pour éditer un groupe, l'Editeur de groupe de ressources s'affiche et comporte les zones suivantes :

Nom du groupe
Le nom du groupe est obligatoire. Vous pouvez modifier un nom de groupe personnalisé existant, et toutes les références à ce groupe sont mises à jour automatiquement lorsque vous sauvegardez vos modifications.

Description du groupe
Facultative pour les groupes personnalisés. Ajoutez une description de l'organisation du groupe. Cette description est affichée dans le Gestionnaire de groupes de ressources.

Affectation de ressource
Tous les systèmes gérés qui sont disponibles pour ajout au groupe sont répertoriés dans la liste d'agent par leur nom de système géré, nom d'hôte, type d'agent et domaine. Vous pouvez cliquer sur un en-tête de colonne pour trier la liste par nom d'agent, nom d'hôte, type ou domaine.

Pour alimenter le groupe, cochez la case correspondant à un ou plusieurs systèmes gérés.

Vous pouvez sélectionner **Afficher uniquement les ressources sélectionnées** afin de masquer les systèmes gérés non affectés.

Si vous avez configuré la Passerelle hybride d'IBM Cloud Application Performance Management, vous pouvez ajouter des systèmes gérés issus de votre domaine IBM Tivoli Monitoring aux groupes de ressources définis par l'utilisateur. Vous ne pouvez ni ajouter des systèmes gérés Tivoli Monitoring aux groupes définis par le système, ni créer de seuils pour ces derniers.

Affectation de seuil

Tous les seuils qui ont été prédéfinis ou ajoutés via le gestionnaire de seuils sont répertoriés dans la liste des seuils par leur nom et leur type d'agent. Vous pouvez cliquer sur l'en-tête d'une colonne pour trier la liste.

Pour ajouter un seuil au groupe, sélectionnez la case à cocher en regard du nom ; pour retirer un seuil du groupe, décochez la case. Pour que le gestionnaire de seuils ajoute ou retire des seuils, vous devez disposer de droits d'affichage. Lorsque vous ajoutez des seuils à un groupe de systèmes, les seuils disponibles sont ceux dont l'ensemble de données est adapté au groupe de systèmes.

Les seuils que vous affectez au groupe sont distribués à chacun des systèmes gérés du groupe de même type d'agent. Même si vous pouvez affecter des seuils de tout type d'agent de surveillance à un groupe, les seuils affectés sont distribués uniquement aux systèmes gérés de même type qui sont membres du groupe. Par exemple, si vous affectez le seuil `MySQL_Process_Down` au groupe, il est inclus dans le groupe, mais n'est distribué qu'aux systèmes gérés par l'Monitoring Agent for MySQL qui appartiennent au groupe.

Vous pouvez sélectionner **Afficher uniquement les seuils sélectionnés** pour masquer les seuils non affectés. Si vous filtrez la liste, cliquez sur dans la zone de filtre pour effacer le filtre et activer la case à cocher.

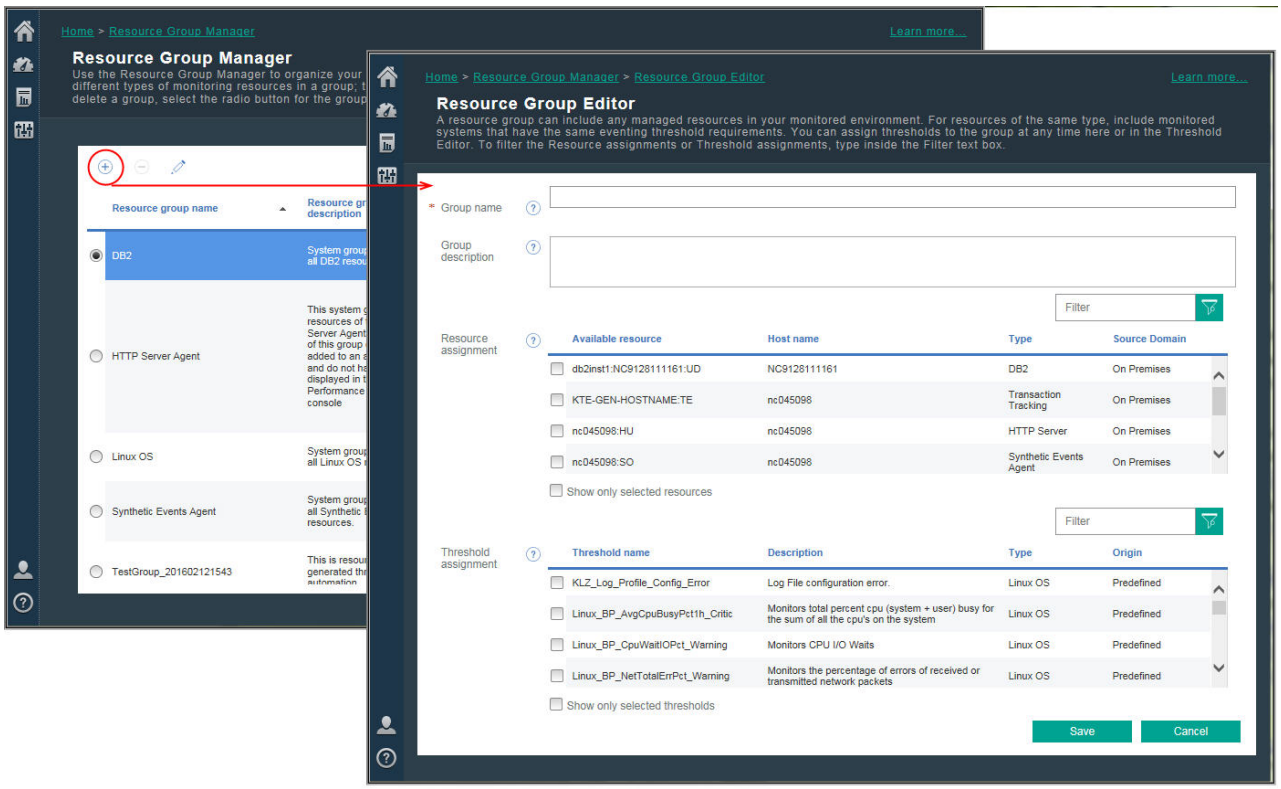
Vous pouvez également affecter un groupe de ressources à un seuil à partir du Gestionnaire de seuils.

Configuration de la notification par courrier électronique

Disponible avec IBM Cloud Application Performance Management : Cliquez sur **Configurer la notification par courrier électronique** pour ouvrir l'application IBM Alert Notification dans un nouvel onglet ou une nouvelle fenêtre de navigation. Utilisez Alert Notification pour créer des utilisateurs et associer leurs adresses électroniques à des groupes de ressources pour que ceux-ci reçoivent des notifications d'événements par courrier électronique.

Avertissement : Si votre navigateur n'autorise pas les fenêtres en incrustation, la fenêtre Alert Notification ne peut pas s'ouvrir. Vous devez configurer le navigateur de manière à autoriser la fenêtre Alert Notification à s'ouvrir pour pouvoir configurer la notification par courrier électronique d'un groupe de ressources.

Lorsque vous cliquez sur **Sauvegarder**, le groupe de ressources est sauvegardé avec la liste des groupes de ressources et apparaît dans le tableau du gestionnaire de groupes de ressources.



Tâches associées:

«Exploration des API», à la page 1115
Utilisez les API IBM Cloud Application Performance Management pour créer des scripts afin d'automatiser l'intégration de votre environnement IBM Cloud Application Performance Management, Private.

Référence associée:

«Gestionnaire de seuils», à la page 1002
Le Gestionnaire de seuils permet de consulter les seuils prédéfinis d'un agent de surveillance et de créer et d'éditer des seuils.

«Gestion des accès utilisateur», à la page 1020
Utilisez la fonction Contrôle d'accès basé sur les rôles de IBM Cloud Application Performance Management pour octroyer aux utilisateurs les droits d'accès dont ils ont besoin pour leur rôle.

Tutoriel : Définition d'un seuil

Les seuils sont le mécanisme d'alerte des problèmes réels et potentiels liés à vos ressources gérées.

Utilisez le tutoriel pour connaître les étapes de base de définition d'un seuil afin de déclencher une alarme lorsque la condition se produit.

Pourquoi et quand exécuter cette tâche

Ce tutoriel s'appuie sur l'agent Linux OS pour montrer comment définir un seuil dans le Gestionnaire de seuils et afficher l'alarme déclenchée dans le Tableau de bord d'Application Performance. Votre ID utilisateur doit disposer du droit d'affichage du Gestionnaire de seuils pour effectuer ces étapes.

Procédure

1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Gestionnaire de seuils**.

2. Cliquez sur la zone de liste **Type de source de données** et sélectionnez le type de données **Linux OS**. Les seuils qui sont définis pour l'agent Linux OS sont affichés dans le tableau.
3. Cliquez sur **Nouveau** pour ouvrir l'éditeur de seuil afin de définir le seuil.
4. Définissez un seuil pour déclencher une alarme de gravité Inconnue lorsque l'UC moyenne est en-dessous de 75 % :
   a. Dans la zone **Nom**, entrez `CPU_average_below_75_percent`.
   b. Dans la zone **Description**, entrez `Tutoriel : Seuils`.
   c. Conservez les valeurs par défaut dans les zones **Gravité**, **Intervalle** et **Echantillons consécutifs requis**.
   d. Dans la zone **Ensemble de données**, sélectionnez **Moyennes UC KLZ**.
   e. Dans la zone **Conditions**, cliquez sur **Nouveau**, puis ajoutez la comparaison dans la boîte de dialogue qui apparaît :
      1) Dans la zone **Attribut**, sélectionnez **CPU_Usage_Current_Average**
      2) Dans la zone **Opérateur**, sélectionnez **Inférieur à**.
      3) Dans la zone **Valeur**, entrez 75.

      Lorsque vous cliquez sur **OK**, l'attribut et la comparaison s'affichent dans la zone **Conditions**.
   f. Dans la zone **Affectation de groupes**, sélectionnez le groupe système **Linux OS**.
   g. Cliquez sur **Sauvegarder** pour terminer la définition et revenir à la page Gestionnaire de seuils.

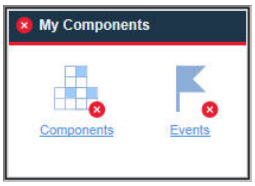
   `CPU_average_below_75_percent` apparaît dans la liste des seuils qui sont définis pour la source de données Linux OS.

Résultats

Vous avez défini un seuil qui déclenche une alarme lorsque l'utilisation de l'UC moyenne sur n'importe lequel de vos systèmes gérés Linux OS est en-dessous de 75 %.

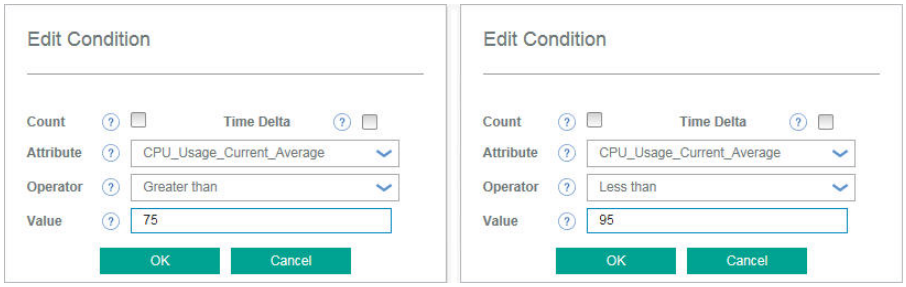
Que faire ensuite

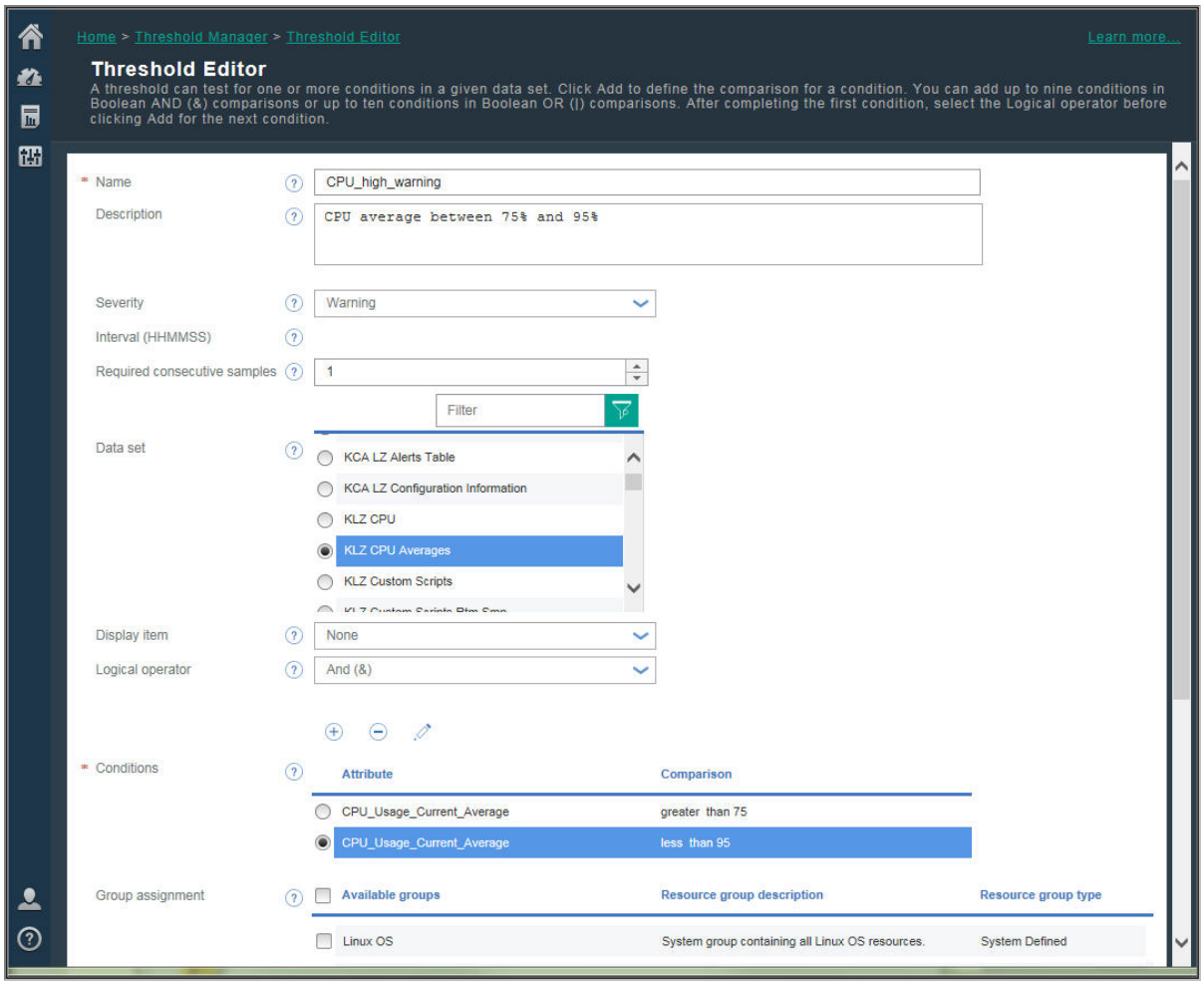
- Affichez l'événement :
  1. Dans la barre de navigation, cliquez sur **Performance** > **Tableau de bord d'Application Performance**.
  2. Dans la zone de récapitulatif Mes composants, cliquez sur le lien **Evénements**.

  3. Dans l'onglet Evénements qui s'ouvre, recherchez le seuil `CPU_average_below_75_percent` dans la liste. Le déclenchement de l'alarme peut prendre 1 ou 2 minutes. Si l'UC moyenne est au-dessus de 75 %, aucune alarme n'est déclenchée.
- Editez le seuil :
  1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Gestionnaire de seuils**.
  2. Cliquez sur la zone de liste **Type de source de données**, puis sélectionnez le type de données **Linux OS**.
  3. Sélectionnez le seuil `CPU_average_below_75_percent` dans la liste, puis cliquez sur **Editer**.
  4. Modifiez l'une des zones d'une condition pour laquelle vous voulez être alerté. Par exemple, vous pouvez changer **Nom** en `CPU_high_warning`, changer **Gravité** en **Avertissement**, remplacer la condition par **Supérieur à 75** et ajouter une condition **Inférieur à 95**. Pour éditer la comparaison, cliquez sur **Editer**, changez **Opérateur** en **Supérieur à** et cliquez sur **OK**. Pour ajouter la

nouvelle condition, laissez la zone **Opérateur logique** définie sur la valeur par défaut **Et (&)**, cliquez sur **Nouveau** pour créer une nouvelle condition, sélectionnez l'**Opérateur Inférieur à**, puis entrez la **Valeur** 95.





- Examinez les seuils prédéfinis pour vos agents et adaptez toutes les valeurs de comparaison en fonction de votre environnement.
- Créez de nouveaux seuils pour déclencher des alarmes sur d'autres conditions dont vous voulez être alerté.

Référence associée:

«Gestionnaire de seuils», à la page 1002
Le Gestionnaire de seuils permet de consulter les seuils prédéfinis d'un agent de surveillance et de créer et d'éditer des seuils.

«Gestion des accès utilisateur», à la page 1020
Utilisez la fonction Contrôle d'accès basé sur les rôles de IBM Cloud Application Performance

Management pour octroyer aux utilisateurs les droits d'accès dont ils ont besoin pour leur rôle.

Tutoriel : Définition d'un seuil pour exécuter une commande sur la ressource gérée

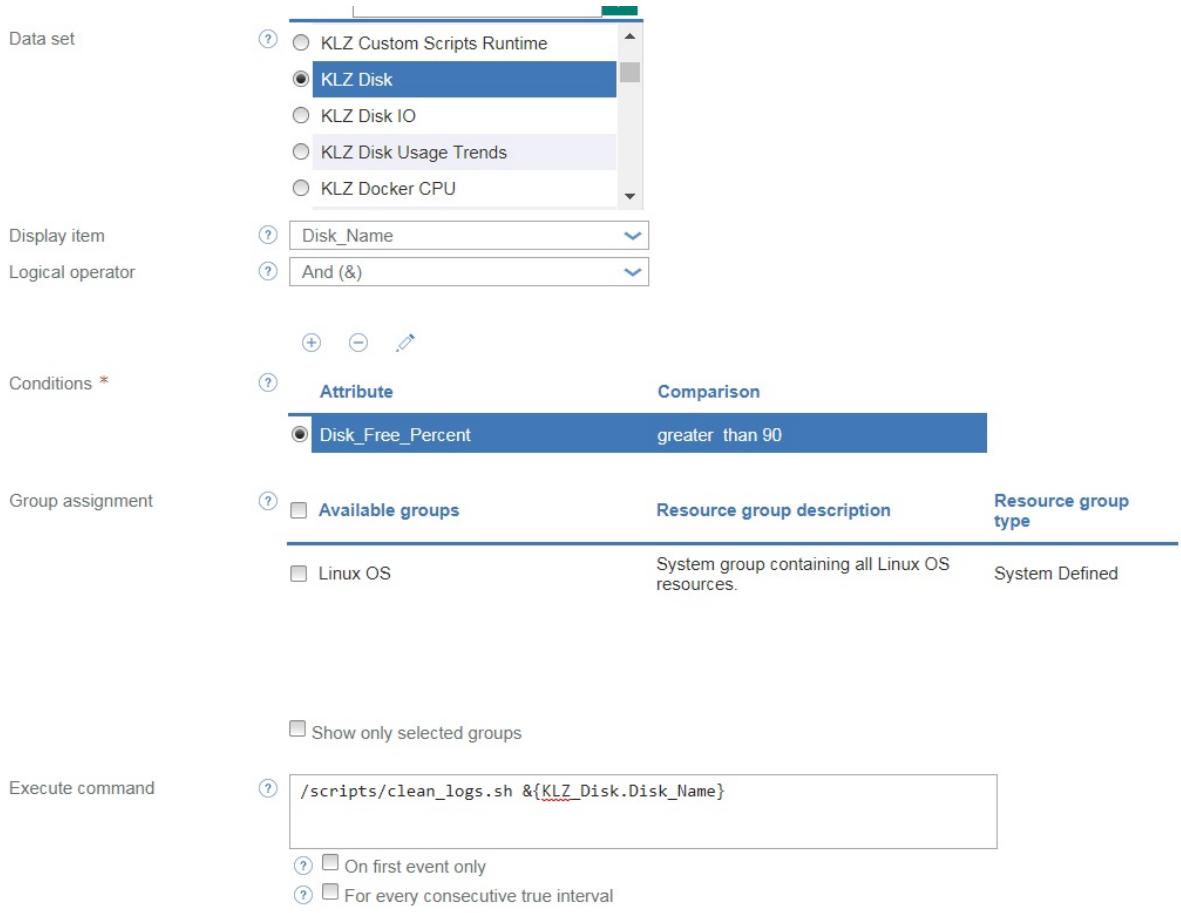
Vous pouvez utiliser l'éditeur de seuil pour transmettre certains paramètres aux agents. Vous avez la possibilité de spécifier les commandes ou un script des commandes qui s'exécuteront automatiquement lors du déclenchement d'un événement.

Pourquoi et quand exécuter cette tâche

Ce tutoriel montre l'utilisation de la zone **Exécuter la commande** pour transmettre un paramètre à votre agent IBM Cloud Application Performance Management.

Procédure

1. Ouvrez le **Gestionnaire de seuils** en cliquant sur **Configuration du système** > **Gestionnaire de seuils**.
2. Sélectionnez *Linux OS* dans la zone **Type de source de données**. Les seuils qui sont définis pour l'agent Linux OS sont affichés dans le tableau.
3. Cliquez sur **Nouveau** pour ouvrir l'éditeur de seuil afin de définir le seuil.
4. Définissez le seuil et les conditions en spécifiant des valeurs pour les différents paramètres tels que **Nom**, **Gravité** et **Conditions**.
5. Sélectionnez *KLZ Disk* dans la zone **Jeu de données**.



6. Entrez la commande suivante dans la zone **Exécuter la commande** :

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

Vous devez remplacer l'espace dans le nom du jeu de données *KLZ Disk* par un trait de soulignement. Le disque *KLZ_Disk.Disk_Name* est transmis dans le script de commandes.

Résultats

Votre script de commandes est configuré pour s'exécuter automatiquement lorsque le seuil défini est atteint. Les commandes sont exécutées sur le système contrôlé pour lequel les événements sont déclenchés.

Référence associée:

«Gestionnaire de seuils»
Le Gestionnaire de seuils permet de consulter les seuils prédéfinis d'un agent de surveillance et de créer et d'éditer des seuils.

Gestionnaire de seuils

Le Gestionnaire de seuils permet de consulter les seuils prédéfinis d'un agent de surveillance et de créer et d'éditer des seuils.

Les seuils sont utilisés pour comparer la valeur d'échantillon d'un attribut avec la valeur définie dans le seuil. Si la valeur d'échantillon satisfait la comparaison, un événement est ouvert. L'événement se ferme automatiquement lorsque la comparaison de seuils n'est plus vraie.

Une fois que vous avez cliqué sur **Configuration du système** > **Gestionnaire de seuils**, la page est affichée avec une table des seuils définis pour le type de source de données sélectionné.

Les types de données qui s'affichent lorsque vous cliquez sur la zone de liste **Type de source de données** sont pour les types d'agents de surveillance et de collecteurs de données installés dans votre environnement géré. Sélectionnez le type de données pour lequel vous souhaitez créer ou afficher des seuils.

Ce tableau répertorie l'ensemble des seuls créées pour le type de données sélectionné et comporte des outils pour la gestion des seuils.

- **Nouveau** ouvre l'éditeur de seuils pour définir un seuil pour le type de données sélectionné.
- Sélectionnez un seuil et cliquez sur **Editer** pour ouvrir l'Editeur de seuils qui permet d'éditer la définition.
- Sélectionnez un seuil dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitez supprimer le seuil, ce dernier est supprimé de la liste et des groupes de ressources auxquels il était affecté. Tous les événements ouverts pour le seuil sont fermés.
- Pour une liste longue, vous pouvez cliquer dans la zone de texte du filtre et taper le début de la valeur du filtre. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour Arrière.

Pour plus d'informations sur les seuils prédéfinis et sur les seuils personnalisés affichés dans le tableau, ainsi que sur la signification de l'affectation de groupe de ressources (ou sur l'absence de signification), voir «Informations de référence», à la page 990. Pour une leçon pratique rapide, voir «Tutoriel : Définition d'un seuil», à la page 998.

Editeur de seuils

Après avoir cliqué sur **Nouveau** ou sélectionné un seuil et cliqué sur **Editer**, l'Editeur de seuils s'affiche et comporte les zones suivantes :

Nom Entrez un nom unique pour le seuil. Ce nom doit commencer par une lettre et peut contenir jusqu'à 31 lettres, nombres et traits de soulignement. Par exemple,

«Average_Processor_Speed_Warning». Le nom du seuil apparaît dans l'onglet Evénements du Tableau de bord d'Application Performance et dans certaines tables du tableau de bord.

Description
Facultatif. La description est utile pour enregistrer l'objectif du seuil que les utilisateurs peuvent voir dans le Gestionnaire de seuils.

Gravité
Sélectionnez la gravité d'événement appropriée dans la liste : Fatal, Critique, Mineur, Avertissement, ou Inconnu.

Les gravités sont consolidées pour être affichées dans le Tableau de bord d'Application Performance : les événements Fatal et Critique sont affichés sous ; les événements Mineur et Avertissement sont affichés sous et les événements Inconnu sont affichés sous (voir «Statut de l'événement», à la page 1156).

Acheminer l'événement de fonction d'intégration d'événements ?
Si vous avez configuré la transmission des événements dans la page **Configuration système** > **Configuration avancée** («Gestionnaire d'événements», à la page 1117), les événements ouverts sont transmis à un récepteur EIF par défaut. Spécifiez la valeur **Non** si vous ne souhaitez pas transmettre les événements de ce seuil à un récepteur EIF.

Pour personnaliser le mappage des seuils aux événements transmis et remplacer ainsi le mappage par défaut entre les seuils et les événements transmis au serveur d'événements, cliquez sur **Personnalisation de l'attribut EIF**. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1007.

Intervalle
Entrez ou sélectionnez le délai d'attente entre les prises d'échantillons de données au format *HHMMSS*, par exemple, 00 15 00 pour 15 minutes. Pour les seuils d'événement échantillonnés, l'intervalle minimum est 000030 (30 secondes) et l'intervalle maximum est 235959 (23 heures, 59 minutes, 59 secondes).

La valeur 000000 (six zéros) indique un seuil d'événement *pur*. Les événements purs sont des notifications non sollicitées. Aucun intervalle d'échantillonnage n'est défini pour les seuils des événements purs et il n'est donc pas possible de surveiller les valeurs en cours d'un indicateur constant. Les événements purs sont fermés après 24 heures ou après la valeur définie dans la zone **Heures avant la fermeture des événements purs** de la page Configuration avancée, catégorie «Gestionnaire d'événements», à la page 1117.

Echantillons consécutifs requis
Indiquez le nombre d'échantillons de seuil consécutifs devant avoir la valeur vrai pour qu'un événement soit généré : lorsqu'un seuil est défini à la valeur 1 et qu'un échantillon est à la valeur vrai, un événement est généré immédiatement. Lorsque le seuil est défini à la valeur 2, deux échantillons de seuil consécutifs doivent avoir la valeur vrai pour qu'un événement soit généré.

Ensemble de données
Sélectionnez l'ensemble de données (groupe d'attributs) pour le type de données à échantillonner. Les attributs disponibles qui peuvent être inclus dans la condition proviennent de l'ensemble de données choisi. Si le seuil comporte plusieurs conditions, ces dernières doivent toutes provenir du même ensemble de données.

Pour obtenir une brève description d'un ensemble de données, déplacez la souris sur son nom. Vous pouvez obtenir la description complète de l'ensemble de données et des attributs en cliquant sur le lien «En savoir plus» de l'infobulle. Vous pouvez également cliquer sur l' **Aide** > **Contenu de l'aide** ou sur l' **Aide** > **Documentation** dans la barre de navigation et ouvrir l'aide ou télécharger Le guide de référence de l'agent de surveillance.

Certains agents sont catégorisés comme agents multinoeuds. Ils possèdent des sous-noeuds pour surveiller plusieurs ressources d'agent. Il se pourrait qu'un agent multinoeud dispose d'ensembles de données qui peuvent être utilisés dans un seuil ; toutefois, tout événement ouvert pour le seuil

ne s'affiche pas dans le Tableau de bord d'Application Performance. Un message vous notifie de la limitation. De tels événements peuvent être transférés au gestionnaire d'événements IBM Netcool/OMNIbus.

Elément affiché
Facultatif. Pour les ensembles de données à plusieurs lignes uniquement. Lorsqu'une évaluation de ligne ouvre un événement, aucun autre événement ne peut être ouvert pour ce seuil sur le système géré jusqu'à ce que l'événement soit fermé. En sélectionnant un élément affiché, vous autorisez le seuil à continuer l'évaluation des autres lignes dans l'échantillon de données et à ouvrir d'autres événements si d'autres lignes sont qualifiées. En outre, l'élément affiché l'est dans l'onglet Evénements du Tableau de bord d'Application Performance pour que vous puissiez facilement distinguer les lignes pour lesquelles des événements ont été ouverts. La liste contient seulement les attributs que vous pouvez désigner comme éléments d'affichage.

Opérateur logique
Ignorez cette zone si votre seuil ne contient qu'une condition. Si vous mesurez plusieurs conditions, sélectionnez l'un des opérateurs suivants avant de cliquer sur **Nouveau** pour ajouter une second, troisième (ou plus) condition :

And (&) si la condition précédente et la condition suivante sont remplies pour que le seuil soit dépassé

Or (|) si une seule de ces conditions doit être remplie pour que le seuil soit dépassé

La combinaison d'opérateurs logiques n'est pas prise en charge. Utilisez tous les opérateurs And ou tous les opérateurs Or. Le seuil peut comporter jusqu'à neuf conditions si l'opérateur Or est utilisé et jusqu'à 10 conditions si l'opérateur And est utilisé.

Si vous utilisez la fonction `Manquant` (décrite plus tard dans la section **Opérateur**), vous ne pouvez utiliser que l'opérateur And dans la formule.

Conditions
La définition de seuil peut inclure logiquement plusieurs seuils ou conditions simultanés.

Cliquez sur **Nouveau** pour ajouter une condition. Sélectionnez une condition et cliquez sur **Editer** pour modifier l'expression ou cliquez sur **Supprimer** pour supprimer l'expression.

Une fois que vous avez cliqué sur **Nouveau** ou **Editer**, renseignez les zones de la boîte de dialogue Ajouter une condition ou Modifier la condition qui s'ouvre :

Nombre
Pour les ensembles de données qui retournent plusieurs lignes pour chaque échantillon de données, vous pouvez comptabiliser chaque ligne qui répond aux critères de la condition. Un événement est ouvert dès que la **Valeur** de comptage est atteinte et que les autres conditions dans la formule sont remplies. Par exemple, si le nombre de processus «zombie» dépasse 10, générez une alerte.

Dans l'exemple suivant, la condition est vraie lorsque plus de 10 lignes sont comptées : **Attribut** Horodatage, **Opérateur** Supérieur à, **Valeur** 10.

Cochez la case **Nombre**, sélectionnez l'**attribut** à comptabiliser, l'**opérateur** relationnelle et la **valeur** de Nombre.Si la formule comporte plusieurs conditions, chacune doit utiliser l'opérateur booléen **And**. Les fonctions **Nombre** et **Delta heure** sont mutuellement exclusives : si vous cochez la case d'une fonction, l'autre est désactivée. L'attribut ne peut correspondre à un identificateur système, tel que Nom de serveur ou ORIGINNODE, être spécifié comme **Elément affiché** ou provenir d'un ensemble de données pour lequel le seuil ouvre des événements purs.

Delta heure
Utilisez la fonction **Delta heure** dans une condition pour comparer l'échantillon d'horodatage (tel que l'heure d'enregistrement) au décalage horaire spécifié.

Une fois que vous avez coché la case **Delta heure**, la zone Delta heure est affichée afin que vous puissiez combiner le signe + (plus) ou - (moins) avec le nombre de jours, d'heures, de minutes ou de secondes. Sélectionnez **Heure d'échantillonnage** ou **Heure spécifique** comme valeur à utiliser dans la comparaison.

Dans l'exemple de journal des événements ci-après, la formule compare l'heure à laquelle l'événement a été consigné à l'horodatage de l'échantillon de données. Si l'événement s'est produit sept jours auparavant, la comparaison est true. Si l'opérateur relationnel était changé en Inférieur ou égal à, la comparaison serait true après 8 jours, 9 jours, etc. :

Attribut : Horodatage

Retardement : -7 jours

Opérateur : Egal à

Valeur : Date de saisie

Attribut

Sélectionnez l'attribut que vous souhaitez comparer dans cette condition. Pour afficher une brève description d'un attribut, déplacez la souris sur son nom dans la liste.

Opérateur

Sélectionnez l'opérateur relationnel pour le type de comparaison :

`Egal`

`Différent`

`Supérieur à`

`Supérieur ou égal à`

`Inférieur à`

`Inférieur ou égal`

`Regular expression contains`

`Regular expression does not contain`

`Regular expression contains` et `Regular expression does not contain` recherchent un critère de concordance dans l'expression. Plus la mise en correspondance d'une chaîne avec l'expression est aisée, plus la charge de travail est efficace au niveau de l'agent. L'expression n'a pas besoin de correspondre à la ligne entière, seulement à la sous-chaîne de l'expression. Par exemple, dans `See him run`, vous voulez savoir si la chaîne contient `him`. Vous pourriez composer l'expression régulière avec `him`, mais vous pourriez également utiliser `.*him.*`. Si vous recherchez `See`, vous pourriez saisir `See`, ou ^`See` pour confirmer qu'il se trouve au début de la ligne. La saisie des caractères génériques `.*` est moins efficace et augmente la charge de travail. Pour plus d'informations sur les expressions régulières, consultez la rubrique developerWorks® technical library ou recherchez `regex` dans votre navigateur.Vous pouvez également sélectionner la fonction `Manquant`, qui compare la valeur de l'attribut spécifié à une liste de valeurs que vous fournissez. La condition prend la valeur True lorsque la valeur ne correspond à aucune valeur de la liste. Cette fonction est utile lorsque vous souhaitez savoir s'il manque quelque chose sur votre système. Conditions et restrictions :

1. L'indicateur sélectionné doit être un attribut de texte : les attributs d'heure et les attributs numériques ne peuvent pas être utilisés.
2. Séparez les valeurs par une virgule (,). Par exemple, `fred,mary,jean`.
3. Vous ne pouvez avoir qu'une seule condition `Manquant` dans un seuil.
4. `Manquant` doit être la dernière condition dans la formule. Si d'autres conditions sont requises, entrez-les avant d'ajouter la fonction Manquant et utilisez uniquement l'opérateur **And (&)** dans la formule. Sinon, toutes les lignes suivantes sont désactivées.

Valeur Entrez la valeur à comparer en utilisant le format autorisé pour l'indicateur, par exemple, 20 pour 20% ou 120 pour 2 minutes.

Affectation de groupes

Affectez un groupe de ressources de sorte que le seuil soit distribué aux systèmes gérés de même type dans le groupe de ressources. Les groupes de ressources disponibles sont les groupes définis par l'utilisateur pour lesquels vous disposez des droits de modification et les groupes de systèmes (pour le type d'agent) pour lesquels vous disposez des droits d'affichage. Les groupes de systèmes disponibles sont également ceux qui sont adaptés à l'ensemble de données sélectionné.

Un seuil auquel aucun groupe n'est affecté n'est distribué à aucun système surveillé et reste arrêté jusqu'à ce qu'il soit distribué à un groupe de ressources.

Un groupe de systèmes, tel que `Linux OS` ou `Serveur HTTP`, distribue le seuil sur tous les systèmes gérés où cet agent est installé. Par défaut, chaque seuil prédéfini est affecté au groupe de systèmes pour cet agent. (Vous pouvez désactiver tous les seuils prédéfinis dans la page Configuration avancée, comme décrit à la section «Activation des seuils», à la page 1121.)

A l'exception des systèmes gérés issus du domaine IBM Tivoli Monitoring : les systèmes gérés issus du domaine Tivoli Monitoring doivent être surveillés et inclure des situations qui ont été distribuées dans votre environnement Tivoli Monitoring.

Pour affecter des groupes au seuil, cochez les cases d'un ou plusieurs groupes de ressources. Si la liste des groupes affectés est longue, vous pouvez sélectionner ☐ **Afficher uniquement les groupes sélectionnés**.

Si vous ne trouvez aucun groupe de ressources auquel vous souhaitez affecter le seuil, vous pouvez sauvegarder la définition de seuil et cliquer sur **OK** lorsque vous êtes invité à confirmer que vous voulez sauvegarder le seuil sans l'affecter à un groupe. Vous pouvez ensuite créer un groupe dans le gestionnaire de groupes de ressources et lui affecter un seuil dans l'Editeur de groupe de ressources. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 995.

Exécution d'une commande

Une fois qu'un événement a été ouvert pour un seuil défini sur true, vous pouvez exécuter automatiquement une commande ou un script de commandes sur le système surveillé pour lequel l'événement a été ouvert. Vous pouvez par exemple vouloir consigner des informations, déclencher un bip audible ou arrêter un travail qui consomme trop ressources.

La commande respecte la syntaxe suivante :

`&{`*`jeu_données.attribut`*`}`

où *jeu_données* est le nom du jeu de données et *attribut* est le nom d'attribut tel qu'affiché dans l'éditeur de seuil. Si le jeu de données ou le nom d'attribut contient un espace, remplacez l'espace par un trait de soulignement.

L'exemple suivant montre comment transmettre le paramètre de nom de disque à une ressource gérée :

```
/scripts/clean_logs.sh &{disque_KLZ.nom_disque}
```

Vous pouvez transférer un ou plusieurs attributs depuis le jeu de données. S'ils sont spécifiés, les attributs multiples sont transférés dans la commande dans l'ordre ($1, $2, etc.).

La commande s'exécute à partir de la ligne de commande avec le même compte utilisateur que celui avec lequel l'agent ou le collecteur d'agent a démarré. Par exemple, si l'agent s'exécute en tant que superutilisateur, le superutilisateur exécute la commande sur le système géré.

Les options suivantes contrôlent la fréquence d'exécution de la commande :

Sélectionnez ☐ **Lors du premier événement uniquement** si l'ensemble de données renvoie plusieurs lignes et que vous souhaitez n'exécuter la commande que pour la première

occurrence de l'événement dans l'échantillon de données. Désélectionnez cette case pour exécuter la commande pour chaque ligne qui génère un événement.

Sélectionnez **Pour chaque intervalle vrai consécutif** pour exécuter la commande chaque fois que le seuil est défini sur true. Désélectionnez cette case pour exécuter la commande lorsque le seuil a la valeur true, mais pas une deuxième fois tant que le seuil n'a pas la valeur false, suivi par une autre évaluation true dans un intervalle ultérieur.

Une fois que vous avez cliqué sur **Sauvegarder**, le seuil est appliqué à tous les systèmes gérés dont le type de données est le même dans les groupes de ressources affectés.

Conseil : Vous pouvez contrôler le comportement de transmission des événements à l'aide des options du **Gestionnaire d'événements** dans la page Configuration avancée. Voir «Configuration avancée», à la page 1117.

Remarque : Pour afficher la liste des attributs qui conviennent à l'inclusion dans la définition de seuil, créez une table avec le fichier que vous prévoyez d'utiliser. .

Concepts associés:

«Informations de référence», à la page 990
Examinez les informations de référence pour en savoir plus sur les seuils, les seuils prédéfinis pour les agents, les groupes de ressources auxquels ils sont affectés et la personnalisation des seuils.

Tâches associées:

«Tutoriel : Définition d'un seuil», à la page 998
Utilisez le tutoriel pour connaître les étapes de base de définition d'un seuil afin de déclencher une alarme lorsque la condition se produit.

«Tutoriel : Définition d'un seuil pour exécuter une commande sur la ressource gérée», à la page 1001
Vous pouvez utiliser l'éditeur de seuil pour transmettre certains paramètres aux agents. Vous avez la possibilité de spécifier les commandes ou un script des commandes qui s'exécuteront automatiquement lors du déclenchement d'un événement.

«Intégration à Netcool/OMNIbus», à la page 905
Vous pouvez réacheminer les événements de IBM Cloud Application Performance Management vers votre gestionnaire d'événements IBM Tivoli Netcool/OMNIbus sur site.

Référence associée:

«Gestion des accès utilisateur», à la page 1020
Utilisez la fonction Contrôle d'accès basé sur les rôles de IBM Cloud Application Performance Management pour octroyer aux utilisateurs les droits d'accès dont ils ont besoin pour leur rôle.

Personnalisation d'un événement à transmettre à un récepteur EIF

Vous pouvez créer des définitions de mappe pour les événements de seuil envoyés au récepteur EIF (Event Integration Facility). Utilisez la fenêtre Personnalisation de l'attribut EIF pour personnaliser le mappage des événements de la fonction d'intégration d'événements transmis et remplacer ainsi le mappage par défaut.

En personnalisant le modèle de message, vous pouvez ajouter des informations sur le problème identifié par l'événement et les données spécifiques de l'événement.

Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser l'emplacement de base de la fonction d'intégration d'événements (EIF), qui est un emplacement *msg* prédéfini envoyant la formule de seuil au récepteur EIF. Vous pouvez également ajouter un ou plusieurs attributs personnalisés de la fonction d'intégration d'événements, ce qui requiert une mise à jour du récepteur EIF et des fichiers de règles de sonde.

Procédure

Pour personnaliser le mappage des événements du seuil actuel aux événements transmis, procédez comme suit :

1. Si le Gestionnaire de seuils n'est pas ouvert, cliquez sur **Configuration du système** > **Gestionnaire de seuils**.
2. Cliquez sur la zone de liste **Type de source de données**, puis sélectionnez le type de données à utiliser.
3. S'il s'agit d'un nouveau seuil, cliquez sur **Nouveau** ; sinon, sélectionnez un seuil et cliquez sur **Editer**.
4. Pour personnaliser le mappage des événements de ce seuil aux événements transmis, vérifiez que **EIF Forwarder** est défini sur `Yes`, cliquez sur **Personnalisation de l'attribut EIF**, puis effectuez l'une des étapes suivantes :
   - **Attributs EIF de base** : pour personnaliser l'emplacement de base, sélectionnez le bouton d'option de **msg** et cliquez sur **Editer**.
   - **Attributs EIF personnalisés** : pour ajouter un emplacement personnalisé, cliquez sur **Ajouter** ; pour éditer un emplacement personnalisé, sélectionnez le bouton d'option de l'emplacement et cliquez sur **Editer**.

   La fenêtre Editer un attribut ou Ajouter un attribut s'ouvre.
5. Renseignez les zones pour personnaliser les valeurs d'emplacement :

Zone	Description	Restriction
Slot name	Nom de l'emplacement de la fonction d'intégration d'événements personnalisé, qui doit commencer par un caractère.	L'emplacement de base de la fonction d'intégration d'événements est **msg** et ne peut pas être modifié.
Slot type	Type d'emplacement personnalisé de la fonction d'intégration d'événements : **String Type** ou **Number Type**.	L'emplacement de base de la fonction d'intégration d'événements est **String Type** et ne peut pas être modifié.
Subtype	Valeur affectée à l'emplacement, qui correspond au type d'emplacement : • **Mapped attribute** active la zone **Mapped attribute** pour ajouter la valeur de l'attribut sélectionné au moment où l'événement se produit • **Literal Value** active la zone **Literal value** pour ajouter du texte au modèle de message • **Literal Value + Mapped Attribute** active les zones **Literal value** et **Mapped attribute** pour ajouter du texte et des valeurs d'attribut au modèle de message et active le bouton **Ajouter** pour ajouter plusieurs valeurs de texte et/ou d'attribut. Un espace est ajouté après chaque valeur littérale ou attribut. Une utilisation type de l'emplacement de base de la fonction d'intégration d'événements **msg** consiste à spécifier une combinaison **Literal Value + Mapped Attribute** pour le modèle de message.	Un emplacement **Number Type** ne peut utiliser que **Mapped Attribute**.

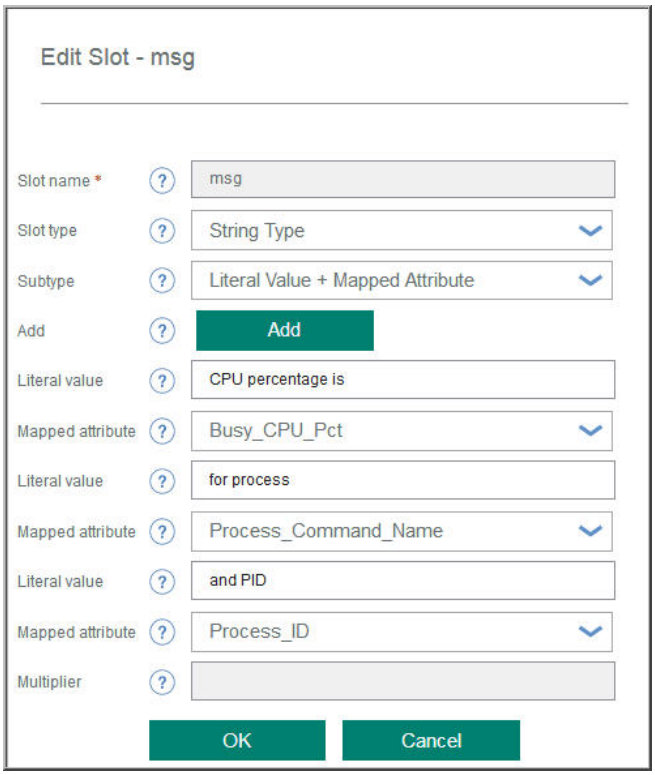
Zone	Description	Restriction
Ajouter	Si vous souhaitez envoyer plusieurs valeurs littérales ou valeurs d'attribut dans le message transmis, cliquez sur **Ajouter** pour ajouter un autre ensemble de zones **Literal value** et **Mapped attribute**. Chaque fois que vous sélectionnez **Ajouter**, ces zones sont ajoutées au panneau. Pour supprimer un ensemble de zones **Literal value** et **Mapped attribute**, effacez le contenu de ces zones avant de cliquer sur **OK**. Voir Exemple.	Activée uniquement si la valeur de **Subtype** est **`Literal Value + Mapped Attribute`**. Six ensembles de zones **Literal value** et **Mapped attribute** au maximum. Si vous ne parvenez pas à voir les zones que vous avez ajoutées, utilisez la fonction de zoom arrière du navigateur (Ctrl -) pour réduire la présentation à la taille de la boîte de dialogue.
Literal value	Texte à inclure dans le modèle de message. Par exemple, la valeur littérale `L'utilisation de la mémoire est élevée à ,` associée à l'attribut mappé **`Utilisation de la mémoire (%)`**, se présente dans l'interface utilisateur Gestionnaire d'événements sous la forme `L'utilisation de la mémoire est élevée à 97,3 %`. Le modèle de message se compose du texte du message fixe et de références de substitution de variable ou de symboles. Le symbole fait référence à des données d'emplacement commun ou d'événement ou à une référence spéciale à la formule de seuil. Les emplacements communs correspondent aux emplacements inclus dans tous les événements transmis, tels que *threshold_name* ; les emplacements d'événement correspondent aux emplacements spécifiques au seuil `msg`.	Désactivée si la valeur de **Subtype** est **`Mapped Attribute`**.
Mapped attribute	Attribut dont vous souhaitez ajouter la valeur au modèle de message. Les attributs disponibles proviennent de l'ensemble de données sélectionné pour le seuil. Par exemple, pour un seuil qui surveille les temps de processeur élevés, vous pouvez mapper l'attribut de pourcentage du temps utilisateur.	Six zones **Mapped attribute** au maximum. Désactivée si la valeur de **Subtype** est **`Literal Value`**. Si la valeur de **Slot type** est **`Number Type`**, seuls les attributs numériques sont disponibles.
Multiplier	Le multiplicateur correspond à la valeur définie une fois que vous avez personnalisé la valeur numérique d'origine de l'attribut mappé par un multiplicateur : valeur de l'emplacement = *attribute1* * *n*. Par exemple, pour convertir les minutes en secondes dans l'événement de la fonction d'intégration d'événements, indiquez un multiplicateur de 60. La valeur du multiplicateur peut être une fraction, exprimée sous forme de valeur décimale, telle que 0.5 ou 5.4.	Activée uniquement pour les attributs numériques (**Slot type** est **`Number Type`**).

Une fois que vous avez cliqué sur **OK** pour fermer la fenêtre, la fenêtre Personnalisation de l'attribut EIF répertorie le nom d'emplacement et indique s'il est personnalisé.

6. Une fois que vous avez terminé d'éditer l'emplacement de base de la fonction d'intégration d'événements ou d'ajouter, de supprimer ou d'éditer des emplacements personnalisés de la fonction d'intégration d'événements pour le seuil, cliquez sur **OK**.
7. Après avoir modifié le seuil, cliquez sur **Sauvegarder**. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1002.

Exemple

Le seuil `Linux_BP_ProcHighCpu_Critical` vérifie si la consommation d'unité centrale est supérieure ou égale à 95 %. Pour ajouter le pourcentage d'unité centrale occupée, le nom de commande du processus et l'ID processus au message récapitulatif, (contenu dans l'emplacement msg), l'emplacement msg a été personnalisé avec trois ensembles de zones **Literal value** et **Mapped attribute** :



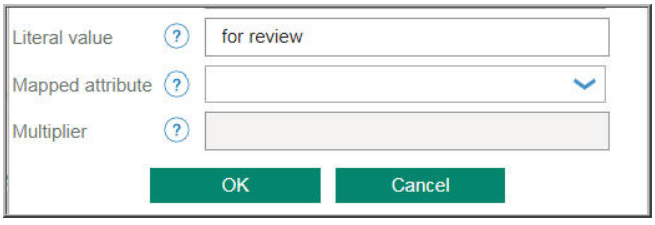
Le modèle de message se présente comme suit :

`CPU percentage is` *`Busy_CPU_Pct`* `for process` *`Process_Command_Name`* `and PID` *`Process_ID`*

Le message résultant affiché dans Event Manager peut se présenter comme suit :

`CPU percentage is` *`97`* `for process` *`large.exe`* `and PID` *`9876`*

Vous pouvez également ajouter les zones **Literal value** et **Mapped attribute** et laisser une zone vide. Par exemple, pour ajouter "for review" au modèle de message, cliquez sur **Ajouter** et entrez `for review` pour **Literal value**.



Le modèle de message se présente maintenant comme suit :

`CPU percentage is` *`Busy_CPU_Pct`* `for process` *`Process_Command_Name`* `and PID` *`Process_ID`* `for review`

Le message résultant affiché dans Event Manager peut se présenter comme suit :

`CPU percentage is` *`96`* `for process` *`big.exe`* `and PID` *`5432`* `for review`

Que faire ensuite

Si vous avez créé des attributs personnalisés de la fonction d'intégration d'événements, vous devez identifier les nouveaux attributs dans la table `alerts.status` sur votre serveur d'objets Netcool/OMNIbus, puis mettre à jour le fichier de configuration `itm_apm_event.rules` qui a été installé au cours de l'intégration de Netcool/OMNIbus avec Cloud APM.

Ajout d'attributs personnalisés EIF à la base de données du serveur d'objets Netcool/OMNIbus

Lorsque vous ajoutez de nouveaux attributs personnalisés EIF pour les seuils, vous devez les identifier dans votre récepteur EIF pour pouvoir afficher les événements transmis qui les utilisent. Si Netcool/OMNIbus est intégré à Cloud APM, mettez à jour la table `alerts.status` pour définir les nouveaux attributs.

Pourquoi et quand exécuter cette tâche

Lorsque vous avez configuré l'intégration de Netcool/OMNIbus à Cloud APM, à l'étape 3, à la page 906, vous avez chargé `itm_apm_db_update.sql`. La procédure ci-après exige que vous utilisiez l'interface interactive SQL pour mettre à jour la table `alerts.status` dans la base de données `itm_apm_db_update.sql`.

Procédure

Suivez cette procédure sur le serveur d'objets Netcool/OMNIbus pour définir les nouveaux attributs personnalisés EIF que vous avez créés dans l'éditeur de seuils :

1. Démarrez l'interface interactive SQL pour modifier la base de données :

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user nom_utilisateur -password mot_de_passe
   -server nom_serveur > itm_apm_db_update.sql
   ```

   Exemple :

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS >
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U nom_utilisateur
   -P mot_de_passe -S nom_serveur
   ```

   Exemple :

   ```
   \temp\apm\itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U smadmin
   -P passw0rd -S NCOMS
   ```

2. Pour chaque emplacement EIF personnalisé, entrez la commande SQL **`ALTER TABLE`** avec le nom d'emplacement personnalisé et le type d'emplacement au format suivant, appuyez sur la touche Entrée, puis entrez `go` et appuyez sur Entrée :

   - Pour un type d'attribut chaîne,

     ```
     alter table alerts.status add nom_attribut_personnalisé varchar(512);
     ```

   - Pour un type d'attribut numérique,

     ```
     alter table alerts.status add nom_attribut_personnalisé integer;
     ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF tel qu'il a été entré dans la zone **slotName** de la fenêtre Ajouter un attribut dans l'éditeur de seuils.

Exemple

L'exemple présente les commandes **`alter table`** permettant d'ajouter les attributs personnalisés **`BusinessApplication`** et **`GenericMetric`**.

```
alter table alerts.status add BusinessApplication varchar(512);
alter table alerts.status add GenericMetric integer;
```

Que faire ensuite

Mettez à jour le fichier de configuration `itm_apm_event.rules` qui a été installé dans le cadre de l'intégration de Netcool/OMNIbus à Cloud APM. Pour plus d'informations, voir «Ajout d'attributs personnalisés EIF aux règles d'événement de récepteur EIF».

Ajout d'attributs personnalisés EIF aux règles d'événement de récepteur EIF

Si vous avez défini de nouveaux attributs personnalisés EIF pour les seuils, vous devez mettre à jour le fichier de règles pour identifier ces nouveaux attributs auprès du récepteur EIF.

Pourquoi et quand exécuter cette tâche

Ces étapes vous amènent à mettre à jour le fichier `itm_apm_event.rules` dans Probe for Tivoli EIF Netcool/OMNIbus afin d'identifier chaque nouvel attribut personnalisé EIF. Si vous utilisez un autre récepteur EIF, mettez à jour les fichiers de règles comme l'exige le récepteur.

Procédure

1. Sur le système où Probe for Tivoli EIF est installé, accédez au répertoire d'installation.

   Linux cd *rép_install*`/tivoli/netcool/omnibus/probes/linux2x86`

   Windows cd *rép_install*`\Tivoli\Netcool\omnibus\probes\win32`

   où *rép_install* est le répertoire par défaut `/opt/IBM/` ou `C:\IBM\` ou le répertoire que vous avez indiqué lors de l'installation de la sonde.
2. Effectuez une copie de sauvegarde du fichier `itm_apm_event.rules`.
3. Ouvrez le fichier Probe for Tivoli EIF `itm_apm_event.rules` dans un éditeur de texte. Le fichier se compose de trois parties que vous modifiez pour ajouter le(s) attribut(s) personnalisé(s) EIF que vous avez créé(s).
4. Ajoutez les instructions **if** avec une nouvelle instruction pour chaque attribut personnalisé EIF qui utilise le format suivant :

   ```
   if(exists($nom_attribut_personnalisé))
   {
    if(regmatch($nom_attribut_personnalisé, "^'.*'$"))
    {
     $SourceType = extract($nom_attribut_personnalisé, "^'(.*)'$")
    }
   }
   ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF tel qu'il a été entré dans la zone **slotName** de la fenêtre Ajouter un attribut.
5. Ajoutez la liste des entrées `@` avec une nouvelle ligne pour chaque attribut personnalisé EIF qui utilise le format suivant :

   ```
   @nom_attribut_personnalisé=$nom_attribut_personnalisé
   ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF.
6. Ajoutez la liste des entrées `$tmpEventData` avec une nouvelle ligne pour chaque attribut personnalisé EIF qui utilise le format suivant :

   ```
   $tmpEventData = nvp_remove( $tmpEventData, "nom_attribut_personnalisé")
   ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF.
7. Sauvegardez et fermez le fichier `itm_apm_event.rules`.
8. Redémarrez Probe for Tivoli EIF pour implémenter vos mises à jour.

Résultats

Le fichier de règles est mis à jour et Probe for Tivoli EIF peut maintenant traiter les événements de seuil qui utilisent les nouveaux attributs personnalisés EIF et transmettent les détails des événements au serveur d'objets Netcool/OMNIbus.

Exemple

Voici un extrait du fichier `itm_apm_event.rules` une fois qu'il a été modifié dans le but d'ajouter ces attributs personnalisés EIF : **`BusinessApplication`** et **`GenericMetric`** (en italique).

```
# ------------------------------------------------------------------
 if(exists($SourceID))
 {
  if(regmatch($SourceID, "^'.*'$"))
  {
   $SourceID = extract($SourceID, "^'(.*)'$")
  }
 }
    ...
    ...
    ...
 if(exists($ManagedSystemGroups))
 {
  if(regmatch($ManagedSystemGroups, "^'.*'$"))
  {
   $SourceType = extract($ManagedSystemGroups, "^'(.*)'$")
  }
 }
 if(exists($BusinessApplication))
 {
  if(regmatch($BusinessApplication, "^'.*'$"))
  {
   $SourceType = extract($BusinessApplication, "^'(.*)'$")
  }
 }
      if(exists($GenericMetric))
 {
  if(regmatch($GenericMetric, "^'.*'$"))
  {
   $SourceType = extract($GenericMetric, "^'(.*)'$")
  }
 }

 @SourceID=$SourceID
 @URL=$ManagementURL
 @Service=$Service
 @SourceType=$SourceType
 @SubscriberID=$TenantID
 @APMHostname=$apm_hostname
 @ManagedSystemGroups=$ManagedSystemGroups
 @BusinessApplication=$BusinessApplication
 @GenericMetric=$GenericMetric

 # ------------------------------------------------------------------
 # -  RTC 66157
 # ------------------------------------------------------------------
 if ( exists ( $appl_label ) )
 {
    if ( match($appl_label, "PI:A:S"))
    {
        @Class = 87723
    }
 }
 # ------------------------------------------------------------------
 # -  RTC 48775 - APM FP5 agents do not populate data in email of EMaaS Basic
```

```
# ------------------------------------------------------------------
if (match( $situation_eventdata, "~" ) )
{
   # Dump all fields into the ITMEventData field
   $tmpEventData = nvp_add($*)
   # Remove the duplicated fields
   $tmpEventData = nvp_remove( $tmpEventData, "appl_label")
   $tmpEventData = nvp_remove( $tmpEventData, "control")
   ...
   ...
   ...
   $tmpEventData = nvp_remove( $tmpEventData, "ManagedSystemGroups")
   $tmpEventData = nvp_remove( $tmpEventData, "EventSeqNo")
   $tmpEventData = nvp_remove( $tmpEventData, "BusinessApplication")
   $tmpEventData = nvp_remove( $tmpEventData, "GenericMetric")
      @ITMEventData = $tmpEventData
```

Utilisation de l'API Resource Group Management Service

Utilisez l'API Resource Group Management Service pour gérer le cycle de vie des groupes de systèmes gérés à partir de la ligne de commande.

Pourquoi et quand exécuter cette tâche

Effectuez des tâches de groupe de ressources telles que la création, l'affichage, la mise à jour et la suppression de groupes de systèmes gérés. Ajoutez et supprimez des systèmes individuels dans les groupes personnalisés. Affichez une liste des systèmes que vous avez ajoutés à un groupe de ressources personnalisées spécifique et qui sont automatiquement ajoutés aux groupes intégrés tels que le groupe de ressources système.

Vous pouvez créer des scripts d'automatisation de tâches telles que la définition de groupes de ressources et l'affectation d'agents à ces groupes. Les groupes de ressources peuvent être des cibles de distributions de seuil et/ou des stratégies de contrôle d'accès.

Dans cette tâche, vous pouvez utiliser des jetons d'accès ou une autorisation de base dans la commande curl :

Jetons d'accès

Utilisez le protocole OIDC (OpenID Connect) pour obtenir un jeton d'accès du serveur OIDC sur le serveur Cloud APM. Le jeton d'accès vous permet d'accéder à l'API pour exécuter des opérations jusqu'à ce que le jeton expire après 30 minutes.

Autorisation de base

Utilisez un outil base64 pour coder l'ID utilisateur et le mot de passe de votre console Cloud APM en une chaîne base64. Le format de la chaîne en entrée est *IDutilisateur:mdp*. Par exemple : `apmadmin:apmpass`. La sortie est une chaîne se présentant comme suit : `YXBtYWRtaW46YXBtcGFzcw==!`.

Utilisez la chaîne `base64_encoded_string` dans l'en-tête d'autorisation de chacune des demandes, comme illustré dans les exemples de commande curl.

Notez que l'ID utilisateur de la console Cloud APM doit être ajouté à un rôle disposant des droits appropriés.

Les opérations suivantes sont décrites dans l'Explorateur d'API et dans la section Exemple qui se trouve à la fin de cette rubrique.

- Renvoyer tous les groupes de ressources ou agents, ou un groupe de ressources ou un agent donné.
- Créer un groupe de ressources personnalisées ou mettre à jour la définition d'un groupe existant.
- Supprimer un groupe de ressources personnalisées spécifié.

- Ajouter des agents à un groupe de ressources personnalisées.
- Supprimer des agents d'un groupe de ressources personnalisées.

La désactivation de l'authentification OIDC, qui est nécessaire avant l'activation de la connexion unique (SSO) entre Cloud APM et d'autres produits IBM tels que Tivoli Common Reporting requérant LTPA pour la connexion unique, n'affecte pas l'API. L'API RESTful continue d'utiliser le serveur OIDC interne de Cloud APM même si OIDC est désactivé pour la connexion unique entre la console Cloud APM et les interfaces utilisateur d'autres produits.

Procédure

Pour définir et modifier des groupes de ressources personnalisées à l'aide de l'API Resource Group Management Service, procédez comme suit. Les agents et groupes de ressources système ne peuvent pas être modifiés.

1. Sur le système où le serveur Cloud APM est installé, ouvrez le fichier suivant, puis copiez l'ID client et le secret client :

   ```
   /opt/ibm/wlp/usr/shared/config/clientSecrets.xml
   ```

   L'exemple suivant montre le contenu du fichier :

   ```
   <server>
     <variable name="client.secret.apmui" value="{xor}J2oZKWQsHXVxeCJwBGsc
   fQ40d2N+cBUPZmltKRNz" />
     <variable name="client.id.apmui" value="rpapmui" />
   </server>
   ```

2. Utilisez un décodeur XOR pour obtenir la valeur réelle du mot de passe. Exemple : `x5Fv;sB*.'}/[4C"Qk(<!/JP962vL`
3. (Facultatif) Si vous prévoyez d'utiliser un jeton d'accès dans votre commande curl, pour obtenir un jeton d'accès, contactez le noeud final du jeton du serveur OIDC en utilisant les quatre paramètres requis : **username**, **password**, **client_id** et **client_secret**. Dans cet exemple de curl, le paramètre **client_secret** a la valeur «secret» :

   ```
   curl --tlsv1.2 -v -k -d «grant_type=password
   &client_id=rpapmui&client_secret=secret
   &username=apmadmin&password=apmpass&scope=openid»
   https://example.mycompany.com:8099/oidc/endpoint/OP/token
   ```

   Output:

   ```
   {"access_token":"jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8",
   "token_type":"Bearer","expires_in":1800,"scope":"openid",
   "refresh_token":"VsCWUhPHBRpidD2F1PVyZ2LNGMuQPTN837t3OoqZj71FcBfsGE"}
   ```

4. (Facultatif) Si vous prévoyez d'utiliser un jeton d'accès dans votre commande curl, extrayez la valeur **access_token**. Si vous examinez le résultat de l'exemple précédent, la valeur est `jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8`.
5. Entrez les demandes à l'API Resource Group Management Service à l'aide d'un jeton d'accès ou d'une autorisation de base.
   Exemple avec jeton d'accès

   ```
   curl --tlsv1.2 -v -k --request GET --url
   'http://myAPMServer.mycompany-domain.com:8090/1.0/topology/mgmt_artifacts'
   --header 'authorization: Bearer  jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8'
   --header 'content-type: application/json'
   ```

   Exemple avec autorisation de base

   ```
   curl --tlsv1.2 -v -k --request GET --url
   'http://myAPMServer.mycompany-domain.com:8090/1.0/topology/mgmt_artifacts'
   --header 'authorization: Basic YXBtYWRtaW46YXBtcGFzcw==!'
   --header 'content-type: application/json'
   ```

6. Pour plus d'informations sur les opérations API, voir la documentation associée dans l'Explorateur d'API. Pour des instructions sur l'accès à l'Explorateur d'API, voir Exploration des API.

   Remarque : Une partie de l'URL et certains des en-têtes présentés dans les exemples sont requis uniquement pour Cloud APM. Par exemple : https://api.ibm.com/perfmgmt/run, x-ibm-service-location, X-IBM-Client-Id, X-IBM-Client-Secret. Voir l'étape 5, à la page 1015 pour des exemples de requête.
7. Vous devez inclure un en-tête de référenceur dans toutes les demandes POST, PUT et DELETE. La valeur de l'en-tête de référenceur est la suivante :

   ```
   -H 'Referer: http://serveur_apm:8090'
   ```

   où *serveur_apm* est l'adresse IP ou le nom d'hôte complet de votre serveur Cloud APM.

Résultats

Les modifications que vous apportez aux groupes de ressources personnalisées dans l'API entrent en vigueur immédiatement et sont affichées dans le Gestionnaire de groupes de ressources (voir «Gestionnaire de groupes de ressources», à la page 995).

Exemple

Cette commande renvoie les noms et les identificateurs uniques de tous les agents :

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_field=keyIndexName
```

Cette commande renvoie une liste de tous les agents de système d'exploitation Linux :

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_filter=description=
"Linux OS"&_field=keyIndexName
```

Cette commande renvoie une liste des groupes de systèmes et des groupes personnalisés :

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes:AgentGroup,
AgentSystemGroup&_field=keyIndexName&_field=displayLabel
```

Cette commande renvoie la liste des agents affectés à un groupe présentant l'identificateur unique {id} :

```
GET /1.0/topology/mgmt_artifacts/{id}/references/to/contains
```

L'exemple suivant utilise la commande curl pour créer un groupe personnalisé.

```
POST /1.0/topology/mgmt_artifacts
```

Remarque : Le corps de la requête POST doit contenir un objet JSON qui définit le groupe tel qu'indiqué par le paramètre **-d**.

```
curl -X POST \
  http://serveur_apm:8090/1.0/topology/mgmt_artifacts \
  -H 'Referer: http://serveur_apm:8090' \
  -H 'authorization: Bearer votre_jeton_d'accès' \
  -H 'content-type: application/json' \
  -d '{
  "keyIndexName": "customGroup",
  "description": "Description du groupe personnalisé",
  "displayLabel": "customGroupLabel",
  "entityTypes": [
    "AgentGroup"
  ],
  "arbitraryStringProperty": "Your custom property value"
}'
```

Cette commande ajoute un agent avec l'identificateur unique {otherid} à un groupe personnalisé présentant l'identificateur unique {id} :

```
POST /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Cette commande supprime un agent avec l'identificateur unique {otherid} d'un groupe personnalisé présentant l'identificateur unique {id} :

```
DELETE /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Utilisation de l'API Threshold Management Service

Utilisez l'API Threshold Management Service pour gérer le cycle de vie de la surveillance des seuils à partir de la ligne de commande.

Pourquoi et quand exécuter cette tâche

Effectuez des tâches du gestionnaire de seuils telles que la création, l'affichage, la mise à jour et la suppression de seuils. Affectez des groupes de ressources à ces seuils. Affichez une liste de l'ensemble des seuils et des affectations de ressources. Affichez une liste de tous les seuils affectés à un groupe de ressources donné.

Vous pouvez créer des scripts d'automatisation de tâches telles que la définition de seuils et l'affectation de ces derniers à des groupes de ressources.

Dans cette tâche, vous pouvez utiliser des jetons d'accès ou une autorisation de base dans la commande curl :

Jetons d'accès

Utilisez le protocole OIDC (OpenID Connect) pour obtenir un jeton d'accès du serveur OIDC sur le serveur Cloud APM. Le jeton d'accès vous permet d'accéder à l'API pour exécuter des opérations jusqu'à ce que le jeton expire après 30 minutes.

Autorisation de base

Utilisez un outil base64 pour coder l'ID utilisateur et le mot de passe de votre console Cloud APM en une chaîne base64. Le format de la chaîne en entrée est *IDutilisateur:mdp*. Par exemple : `apmadmin:apmpass`. La sortie est une chaîne se présentant comme suit : `YXBtYWRtaW46YXBtcGFzcw==!`.

Utilisez la chaîne `base64_encoded_string` dans l'en-tête d'autorisation de chacune des demandes, comme illustré dans les exemples de commande curl.

Notez que l'ID utilisateur de la console Cloud APM doit être ajouté à un rôle disposant des droits appropriés.

Les opérations suivantes sont décrites dans l'Explorateur d'API et dans la section Exemple qui se trouve à la fin de cette rubrique.

- Renvoyer tous les seuils ou obtenir un seuil spécifique. Vous pouvez filtrer la demande avec ces attributs : **`label`**, qui correspond au nom de seuil, **`_appliesToAgentType`**, qui correspond à un code produit de 2 caractères, et **`_uiThresholdType`**, qui correspond au type de seuil qui est affiché dans les pages Gestionnaire de seuils et Editeur de groupe de ressources de la console Cloud APM. Vous pouvez utiliser **`_offset`** ou **`_limit`** lorsque vous obtenez les seuils
- Créer un seuil ou mettre à jour la définition d'un seuil existant. Vous devez inclure l'en-tête X-HTTP-Method-Override réglé sur PATCH pour la demande de mise à jour
- Supprimer un seuil spécifié
- Renvoyer toutes les affectations de ressources ou une affectation de ressource spécifique qui montre les seuils affectés à chaque groupe de ressources. Vous pouvez filtrer la demande avec ces attributs : **`resource._id`** et **`threshold._id`** ; et utilisez ces opérateurs **`=`** (égal) et **`!=`** (non égal) pris en charge
- Créer une affectation de ressources qui affecte un seuil unique à un groupe de ressources unique

- Supprimer une affectation de ressources, ce qui supprime un seuil unique à partir d'un seul groupe de ressources

La désactivation de l'authentification OIDC, qui est nécessaire avant l'activation de la connexion unique (SSO) entre Cloud APM et d'autres produits IBM tels que Tivoli Common Reporting requérant LTPA pour la connexion unique, n'affecte pas l'API. L'API RESTful continue d'utiliser le serveur OIDC interne de Cloud APM même si OIDC est désactivé pour la connexion unique entre la console Cloud APM et les interfaces utilisateur d'autres produits.

Procédure

1. Sur le système où le serveur Cloud APM est installé, ouvrez le fichier suivant, puis copiez l'ID client et le secret client :

   ```
   /opt/ibm/wlp/usr/shared/config/clientSecrets.xml
   ```

   L'exemple suivant montre le contenu du fichier :

   ```
   <server>
     <variable name="client.secret.apmui" value="{xor}J2oZKWQsHXVxeCJwBGsc
   fQ40d2N+cBUPZmltKRNz" />
     <variable name="client.id.apmui" value="rpapmui" />
   </server>
   ```

2. Utilisez un décodeur XOR pour obtenir la valeur réelle du mot de passe. Exemple : `x5Fv;sB*.'}/[4C"Qk(<!/JP962vL`
3. (Facultatif) Si vous prévoyez d'utiliser un jeton d'accès dans votre commande curl, pour obtenir un jeton d'accès, contactez le noeud final du jeton du serveur OIDC en utilisant les quatre paramètres requis : **username**, **password**, **client_id** et **client_secret**. Dans cet exemple de curl, le paramètre **client_secret** a la valeur «secret» :

   ```
   curl --tlsv1.2 -v -k -d «grant_type=password
   &client_id=rpapmui&client_secret=secret
   &username=apmadmin&password=apmpass&scope=openid»
   https://example.mycompany.com:8099/oidc/endpoint/OP/token
   ```

   Output:

   ```
   {"access_token":"jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8",
   "token_type":"Bearer","expires_in":1800,"scope":"openid",
   "refresh_token":"VsCWUhPHBRpidD2F1PVyZ2LNGMuQPTN837t3OoqZj71FcBfsGE"}
   ```

4. (Facultatif) Si vous prévoyez d'utiliser un jeton d'accès dans votre commande curl, extrayez la valeur **access_token**. Si vous examinez le résultat de l'exemple précédent, la valeur est `jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8`.
5. Entrez les demandes à l'API Threshold Management Service à l'aide d'un jeton d'accès ou d'une autorisation de base.
   Exemple avec jeton d'accès

   ```
   curl --tlsv1.2 -v -k --request GET
   --url 'https://myAPMServer.mycompany-domain.com:8091/1.0/thresholdmgmt/
   threshold_types/itm_private_situation/thresholds'
   --header 'authorization: Bearer  jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8'
   --header 'content-type: application/json'
   ```

   Exemple avec autorisation de base

   ```
   curl --tlsv1.2 -v -k --request GET
   --url 'https://myAPMServer.mycompany-domain.com:8091/1.0/thresholdmgmt/
   threshold_types/itm_private_situation/thresholds'
   --header 'authorization: Basic YXBtYWRtaW46YXBtcGFzcw==!' --header
   'content-type: application/json'
   ```

6. Pour plus d'informations sur les opérations API, voir la documentation associée dans l'Explorateur d'API. Pour des instructions sur l'accès à l'Explorateur d'API, voir Exploration des API.

Remarque : Une partie de l'URL et certains des en-têtes illustrés dans les exemples ne sont requis que pour Cloud APM. Par exemple : https://api.ibm.com/perfmgmt/run, x-ibm-service-location, X-IBM-Client-Id, X-IBM-Client-Secret. Voir l'étape 5, à la page 1018 pour des exemples de requête.

Exemple

Cette commande renvoie tous les seuils qui sont inscrits sur le serveur :

```
GET /threshold_types/itm_private_situation/thresholds
```

Cette commande renvoie les informations pour le seuil avec l'étiquette (nom) `Mon_seuil`.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=label%3DMon_seuil
```

Cette commande renvoie tous les seuils pour le type d'agent `LZ`, qui est le code composant pour l'Agent Linux OS.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=_appliesToAgentType%3DLZ
```

Cette commande a la même sortie que la commande précédente, mais le nom de l'agent est donné tel qu'il apparaît dans la console Cloud APM.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=_uiThresholdType%3DLinux OS
```

Cette commande renvoie tous les groupes de ressources auxquels le seuil `123` est affecté :

```
GET /resource_assignments?_filter=threshold._id=123
```

L'exemple suivant utilise la commande curl pour créer un seuil.

```
POST /1.0/thresholdmgmt/threshold_types/itm_private_situation/thresholds
```

A faire : Le corps de la requête POST doit contenir un objet JSON qui définit le seuil tel qu'indiqué par le paramètre **-d**. Exemple :

```
curl -X POST\
 https://serveur_apm:8091/1.0/thresholdmgmt/threshold_types/itm_private_situation/thresholds \
  -H 'authorization: Bearer votre_jeton_d'accès' \
  -H 'content-type: application/json' \
  -d '{
  "label": "Nom_de_votre_seuil_Linux",
  "description": "Définition de votre seuil Linux",
  "configuration": {
    "type": "json",
    "payload": {
      "formulaElements": [
        {
          "function": "*MKTIME",
          "metricName": "KLZ_CPU.Timestamp",
          "operator": "*EQ",
          "threshold": "1455767100000",
          "timeDelta": {
            "operator": "+",
            "delta": "3",
            "unit": "Hours"
          }
        }
      ,
      "period": "011500",
      "periods": "3",
      "severity": "Fatal",
      "matchBy": "KLZCPU.CPUID",
      "operator": "*OR",
      "actions": [
        {
          "name": "command",
          "command": "ps -ef",
```

```
          "commandFrequency": "Y",
          "commandWhen": "Y",
          "commandWhere": "N"
        }
      ]
    }
  }
}
]'
```

Gestion des accès utilisateur

Utilisez la fonction Contrôle d'accès basé sur les rôles de IBM Cloud Application Performance Management pour octroyer aux utilisateurs les droits d'accès dont ils ont besoin pour leur rôle.

La sécurité dans Cloud APM est basée sur les rôles. Un rôle est un groupe de droits qui contrôle les actions que vous pouvez effectuer dans Cloud APM. Vous pouvez créer des rôles personnalisés dans Cloud APM. Vous pouvez affecter des droits à des rôles personnalisés ou davantage de droits aux rôles par défaut existants. Vous pouvez affecter des utilisateurs et des groupes d'utilisateurs à des rôles par défaut existants ou à des rôles personnalisés. Vous pouvez affecter des utilisateurs et des groupes d'utilisateurs à plusieurs rôles. Les droits sont cumulatifs, un utilisateur ou un groupe est affecté à tous les droits de tous les rôles auxquels il est affecté.

Si vous n'êtes pas membre d'un rôle et que vous essayez de vous connecter à Cloud APM, le message **Non autorisé** apparaît.

Cloud APM utilise le registre de base des profils Liberty de WebSphere Application Server comme méthode par défaut pour l'authentification d'utilisateur. Vous pouvez également utiliser un registre LDAP à cet effet.

L'utilisateur par défaut est apmadmin. L'utilisateur apmadmin est par défaut membre du rôle Administrateur de rôles. L'utilisateur apmadmin est ajouté au registre de base lors de l'installation et vous pouvez en ajouter d'autres. Pour plus d'informations, voir «Gestion des accès utilisateur».

Remarque : Cette configuration ne s'applique qu'aux environnements de test et de démonstration, car le registre de base ne permet ni de verrouiller les comptes utilisateur, ni de contrôler l'expiration des mots de passe utilisateur. Un serveur LDAP fournit des contrôles de sécurité supplémentaires. Pour les environnements de production, il est recommandé de configurer Cloud APM de sorte à utiliser un serveur LDAP pour l'authentification à la place du registre de base. Pour plus d'informations, voir «Intégration à LDAP», à la page 931.

Authentification d'utilisateur à l'aide du registre de base des profils Liberty de WebSphere Application Server

Si vous utilisez le registre de base des profils Liberty de WebSphere Application Server pour l'authentification des utilisateurs, effectuez les étapes suivantes :

1. Créez des utilisateurs et des groupes d'utilisateurs dans ce registre d'utilisateurs de base. Le fichier `basicRegistry.xml` est disponible dans le répertoire `/opt/ibm/wlp/usr/shared/config`. Le fichier `basicRegistry.xml` possède un attribut id et un attribut name pour chaque entrée d'utilisateur. Cloud APM n'utilise que la valeur de l'attribut name. Il est recommandé de définir ces deux attributs sur la même valeur afin d'éviter toute confusion. Pour plus d'informations sur la configuration du registre d'utilisateurs de base avec un profil Liberty, voir l'exemple Utilisation de BasicRegistry et du mappage de rôle sur Liberty dans WebSphere Application Server Knowledge Center
2. Dans Cloud APM, utilisez la page Contrôle d'accès basé sur les rôles pour affecter à des utilisateurs et des groupes d'utilisateurs des rôles par défaut et personnalisés. Pour plus d'informations sur l'utilisation des rôles, voir «Rôles et droits», à la page 1021.

Remarque : Si vous rencontrez des problèmes lors de l'ajout d'utilisateurs à des groupes, redémarrez le serveur OIDC à l'aide de la commande **apm restart oidc**. Pour plus d'informations sur le démarrage des services, voir «Démarrage, arrêt et vérification du statut des composants serveur», à la page 1090.

Authentification d'utilisateur à l'aide du registre LDAP

1. Configurez Cloud APM pour l'intégrer à votre référentiel LDAP. Pour plus d'informations, voir «Intégration à LDAP», à la page 931.
2. Créez des utilisateurs et des groupes d'utilisateurs dans votre référentiel LDAP. Pour plus d'informations sur la configuration d'un registre LDAP avec le profil Liberty, voir Utilisation de BasicRegistry et du mappage de rôle sur Liberty
3. Remplacez l'utilisateur par défaut par un utilisateur LDAP. Pour plus d'informations, voir «Modification de l'utilisateur apmadmin par défaut», à la page 937.
4. Dans Cloud APM, utilisez la page Contrôle d'accès basé sur les rôles pour affecter à des utilisateurs et des groupes d'utilisateurs des rôles par défaut et personnalisés. Pour plus d'informations sur l'utilisation des rôles, voir «Rôles et droits».

Si vous n'êtes pas membre d'un rôle et que vous essayez de vous connecter à Cloud APM, le message **Non autorisé** apparaît.

Rôles et droits

Un *rôle* est un groupe de droits qui contrôle les actions que vous pouvez effectuer dans Cloud APM.

Utilisez la page Contrôle d'accès à base de rôles pour gérer les utilisateurs et les rôles ou utilisez l'API d'autorisation pour effectuer des tâches de contrôle d'accès basé sur les rôles à partir de la ligne de commande. Pour plus d'informations, voir «Exploration des API», à la page 1115.

Il existe quatre rôles par défaut disponibles dans Cloud APM :

Administrateur de rôles
Ce rôle est destiné aux utilisateurs dont la fonction principale est de créer des règles de contrôle d'accès pour Cloud APM. Ce rôle possède tous les droits. Si vous modifiez l'utilisateur par défaut, le nouvel utilisateur par défaut est automatiquement membre du rôle Administrateur des rôles. Ce rôle ne peut pas être édité. Les administrateurs de rôles ne peuvent pas se supprimer eux-mêmes du rôle Administrateur des rôles. Cette restriction supprime le risque de supprimer accidentellement tous les utilisateurs du rôle Administrateur des rôles.

Administrateur de surveillance
Ce rôle est destiné aux utilisateurs dont la fonction principale est d'utiliser Cloud APM pour surveiller les systèmes. Les administrateurs de surveillance effectuent des tâches telles que l'ajout d'applications de surveillance, la création de seuils, l'ajout de groupes de ressources et la distribution des seuils à ces groupes de ressources. Ce rôle peut être édité.

Administrateur système
Ce rôle est destiné aux utilisateurs dont la fonction principale est d'effectuer des tâches d'administration pour le système Cloud APM. Les administrateurs système effectuent des tâches telles que la configuration du gestionnaire d'événements ou la configuration de la passerelle hybride. Ce rôle peut être édité.

Utilisateur de surveillance
Ce rôle est destiné aux utilisateurs dont la fonction principale est de configurer et gérer la santé et l'état des systèmes surveillés par Cloud APM. Ce rôle peut être édité.

Le tableau suivant décrit les droits que vous pouvez affecter aux rôles, ainsi que les quatre rôles par défaut disponibles et les droits associés :

Tableau 203. Rôles et droits.

	Administrateur de rôles		Administrateur de surveillance		Administrateur système		Utilisateur de surveillance	
	Afficher	**Modifier**	**Afficher**	**Modifier**	**Afficher**	**Modifier**	**Afficher**	**Modifier**
Droits d'accès de la configuration système								
Configuration avancée	✓	N/A	—	N/A	✓	N/A	—	N/A
Configuration d'agent	✓	N/A	✓	N/A	—	N/A	—	N/A
Pages d'information	✓	N/A	✓	N/A	✓	N/A	✓	N/A
Fournisseur de recherche	✓	N/A	✓	N/A	—	N/A	—	N/A
Statistiques d'utilisation (voir la remarque)	✓	N/A	✓	N/A	—	N/A	—	N/A
Droits d'accès aux ressources								
Tableau de bord des performances des applications	✓	✓	✓	✓	✓	—	✓	—
Applications	✓	✓	✓	✓	—	—	✓	—
Application individuelle	«Droits des groupes d'applications et de ressources», à la page 1024.							
Tableau de bord de diagnostic	✓	N/A	✓	N/A	—	N/A	✓	N/A
Gestionnaire de groupes de ressources	✓	N/A	✓	N/A	—	N/A	—	N/A
Groupe de ressources individuelles	«Droits des groupes d'applications et de ressources», à la page 1024.							
Groupes de ressources	✓	✓	✓	✓	—	—	—	—
Synthetic Script Manager	✓	N/A	✓	N/A	✓	N/A	—	N/A
Gestionnaire de seuils	✓	N/A	✓	N/A	—	N/A	—	N/A

Où ✓ indique que les membres de ce rôle disposent de ces droits.

— indique que les membres de ce rôle ne disposent pas de ces droits.

N/A indique ces droits n'existent pas

Remarque : Bien que les **`Statistiques d'utilisation`** soient affichées dans la liste des **Droits de la configuration système**, elles ne sont plus applicables à Cloud APM.

Le tableau suivant décrit les actions associées à chacun des droits :

Tableau 204. Droits.

Droit	Description
Configuration avancée	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher >**Configuration avancée** dans la barre de menu. • Effectuer et sauvegarder des modifications dans la fenêtre **Configuration avancée**. • Afficher >**Gestionnaire de passerelle hybride** dans la barre de menu. • Effectuer et sauvegarder des modifications dans la fenêtre **Gestionnaire de passerelle hybride**.
Configuration d'agent	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher >**Configuration d'agent** dans la barre de menu. • Effectuer et sauvegarder des modifications dans la fenêtre **Configuration d'agent**.

Tableau 204. Droits (suite).

Droit	Description
Pages d'information	Si vous disposez des droits d'affichage, vous pouvez effectuer la tâche suivante : • Afficher les icônes Mise en route et Aide dans la barre de menus. **Remarque :** Lorsque la page **Mise en route** s'ouvre, si vous désélectionnez **Afficher cette page au démarrage**, une erreur de refus de droits s'affiche pour les connexions ultérieures. Cependant, vous pourrez toujours accéder à la page **Mise en route** et aux autres sections auxquelles vous êtes autorisé à accéder.
Fournisseur de recherche	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher >**Configurer des fournisseurs de recherche** dans la barre de menu. • Effectuer et sauvegarder des modifications dans la page **Configurer des fournisseurs de recherche**.
Tableau de bord des performances des applications	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher l'icône dans la barre de menu. • Afficher le Tableau de bord d'Application Performance. • Ouvrir des pages personnalisées du tableau de bord dans l'onglet Vues personnalisées. • Créer des vues dans l'onglet Détails d'attribut et les sauvegarder pour votre propre usage. Si vous disposez des droits de modification, vous pouvez effectuer les tâches suivantes : • Afficher l'icône dans la barre de menu. • Afficher le Tableau de bord d'Application Performance. • Créer et sauvegarder des pages personnalisées du tableau de bord dans l'onglet Vues personnalisées. • Créer des vues dans l'onglet Détails d'attribut et les partager avec d'autres utilisateurs. • Afficher l'option **Actions**>**Editer** dans les pages de composants ; cette option vous permet d'éditer les valeurs de seuil ainsi que d'autres paramètres des widgets de groupe qui affichent le tableau de bord Composants.
Applications	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher des applications dans le Tableau de bord des applications. Si vous disposez des droits de modification, vous pouvez effectuer les tâches suivantes : • Afficher des applications dans le Tableau de bord des applications • Créer, modifier et supprimer des applications ; les icônes apparaissent dans le Tableau de bord des applications.
Application individuelle	Voir «Droits des groupes d'applications et de ressources», à la page 1024.
Gestionnaire de groupes de ressources	Si vous disposez des droits d'affichage, vous pouvez effectuer la tâche suivante : • Afficher >**Gestionnaire de groupes de ressources** dans la barre de menu.

Tableau 204. Droits (suite).

Droit	Description
Groupes de ressources	Si vous disposez des droits d'affichage, vous pouvez effectuer la tâche suivante : • Afficher les groupes de ressources et les systèmes qui y résident dans le gestionnaire de groupes de ressources. Pour affecter des seuils, vous devez également être membre d'un rôle qui dispose du droit d'affichage du Gestionnaire de seuils. Si vous disposez des droits de modification, vous pouvez effectuer les tâches suivantes : • Afficher les groupes de ressources et leur contenu dans le Gestionnaire de groupes de ressources. • Créer, modifier et supprimer des groupes de ressources. Les icônes ⊕ ⊖ ✎ sont visibles dans le gestionnaire de groupes de ressources. **Remarque :** Le Gestionnaire de groupes de ressources permet d'organiser les systèmes surveillés en groupes, afin que des seuils de génération d'événement puissent être affectés à ces groupes. Si vous ne disposez pas des droits d'affichage pour le gestionnaire de seuils, vous ne pourrez pas voir les seuils de génération d'événement affectés aux groupes de ressources. Si vous affectez le droit de modification des groupes de ressources à un rôle, vous devez également affecter le droit d'affichage du gestionnaire de seuils au rôle.
Groupe de ressources individuelles	Voir «Droits des groupes d'applications et de ressources».
Gestionnaire de seuils	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher >**Gestionnaire de seuils** dans la barre de menu. • Créer, modifier et supprimer des seuils dans le gestionnaire de seuils. • Afficher et éditer l'affectation des groupes de ressources pour les seuils dans le gestionnaire de seuils si vous disposez des droits appropriés pour le ou les groupes de ressources. • Afficher et éditer éventuellement l'affectation des seuils des groupes de ressources dans le gestionnaire de groupes de ressources si vous disposez des droits appropriés pour le gestionnaire de groupes de ressources et pour le ou les groupes de ressources et afficher les droits du gestionnaire de seuils.
Synthetic Script Manager	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Créer, modifier et supprimer des transactions synthétiques dans Synthetic Transaction Manager. **Remarque :** Pour utiliser des transactions synthétiques dans Synthetic Transaction Manager, vous devez également être membre d'un rôle qui dispose du droit d'affichage pour **Configuration d'agent**.
Tableau de bord de diagnostic	Si vous disposez des droits d'affichage, le bouton Diagnostiquer apparaît dans les tableaux de bord de diagnostic de l'Agent WebSphere Applications, de l'Agent Node.js, de l'Agent Ruby et de l'agent Microsoft .NET. Cliquez sur le bouton Diagnostiquer pour accéder aux tableaux de bord de diagnostic.

Droits des groupes d'applications et de ressources

Vous pouvez attribuer des droits à des groupes d'applications et de ressources individuels.

Droits relatifs aux applications

Dans Cloud APM, une application est constituée d'un groupe de composants et des instances qui résident dans ces composants. Utilisez la fenêtre Ajouter une application pour définir une application. Pour plus d'informations sur la définition d'une application, voir Gestion des applications.

Deux types de droits sont disponibles pour une application individuelle : affichage et modification. Si une application est renommée, les droits ne sont pas conservés. Vous devez réaffecter les droits d'affichage et de modification.

Affichage

Le droit d'affichage pour une application est prioritaire sur tout autre type de droit. Pour afficher une application, il n'est pas nécessaire d'être membre d'un rôle qui dispose du droit d'affichage pour chaque composant et instance de composant de l'application. Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit d'affichage pour une application :

Tableau 205. Droits d'affichage pour une application

Action	Droits disponibles
Afficher tous les composants de prise en charge dans cette application.	✓
Afficher l'application et ses composants dans l'arborescence.	✓
Afficher les composants de l'application dans Mes composants.	✓
Afficher les pages de tableau de bord personnalisées associées à l'application.	✓
Ajouter ou supprimer des composants de l'application.	–
Affecter des seuils aux composants des applications.	–
Afficher les composants de prise en charge d'une application dans le gestionnaire de groupes de ressources.	–

Modification

Si vous êtes membre d'un rôle qui dispose des droits de modification pour une application individuelle, vous pouvez :

- Supprimer l'application.
- Créer des pages de tableau de bord personnalisées dans l'onglet Vues personnalisées. Voir «Vues personnalisées», à la page 1160.
- Ajouter ou retirer des composants et des instances de composant à l'aide de la fenêtre Modifier une application. Les composants et les instances de composant disponibles pour vous dans la fenêtre Modifier une application sont filtrés en fonction des droits de votre rôle. Les composants suivants sont disponibles :
  - Les composants sur lesquels vous avez directement des droits d'accès dans les groupes de ressources système et le groupe de ressources personnalisées
  - Les composants dont vous avez indirectement hérité les autorisations basées sur d'autres applications sur lesquelles vous disposez d'une autorisation de modification

Droits relatifs à un groupe de ressources

Utilisez les groupes de ressources pour regrouper des composants par type ou par objectif. Pour plus d'informations sur la création de groupes de ressources, voir «Gestionnaire de groupes de ressources», à la page 995.

Il existe deux types de groupe de ressources différents : les groupes de ressources personnalisées et les groupes de ressources système.

Groupes de ressources définies personnalisées

Créez des groupes de ressources personnalisées dans le gestionnaire de groupes de ressources. Les groupes de ressources personnalisées permettent de regrouper des ressources en fonction de leur objectif.

Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit d'affichage pour un groupe de ressources personnalisées :

Tableau 206. Droits d'affichage pour un groupe de ressources personnalisées

Action	Droits disponibles
Afficher le groupe de ressources personnalisées et les ressources de ce groupe dans le gestionnaire de groupes de ressources.	✓
Afficher des ressources qui font partie du groupe de ressources personnalisées dans la fenêtre Ajouter une application.	✓
Ajouter des ressources dans le groupe de ressources personnalisées.	—
Supprimer des ressources du groupe de ressources personnalisées.	—

Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit de modification pour un groupe de ressources personnalisées :

Tableau 207. Droits de modification pour un groupe de ressources personnalisées

Action	Droits disponibles
Affecter des seuils au groupe de ressources personnalisées dans l'éditeur de seuils. **Remarque :** Pour affecter des seuils, vous devez également être membre d'un rôle qui dispose du droit d'affichage pour l'éditeur de seuils.	✓
Ajouter des ressources dans le groupe de ressources personnalisées.	✓
Supprimer des ressources du groupe de ressources personnalisées.	✓

Groupes de ressources système

Les groupes de ressources système sont définis automatiquement dans le cadre de la configuration de l'environnement Cloud APM. Les groupes de ressources système ne peuvent pas être créés, supprimés ou modifiés manuellement. Seul le droit d'affichage est disponible pour les groupes de ressources système ; le droit de modification n'est pas disponible.

Des groupes de ressources système sont définis pour chaque type de ressource au moment où la ressource est reconnue par le serveur Cloud APM. Un groupe de ressources système existe pour chaque type de ressource connecté au serveur Cloud APM.

Les agents Cloud APM sont un exemple d'une ressource. Par exemple, la première fois que vous téléchargez, installez et démarrez un agent Db2, un groupe de ressources système nommé Db2 est créé. Ce groupe contient tous les agents Db2 qui seront ultérieurement ajoutés à l'environnement Performance Management.

Le groupe de ressources système de chaque type de ressource contient toutes les ressources de ce type, y compris les ressources IBM Tivoli Monitoring. Si votre environnement dispose à la fois d'IBM Tivoli Monitoring et d'IBM Cloud Application Performance Management, vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management afin d'offrir

une vue des agents des deux domaines. Les groupes de ressources définis par le système contiennent des agents des deux domaines. Pour plus d'informations, voir «Intégration à IBM Tivoli Monitoring V6.3», à la page 871.

Certains groupes de ressources système sont basés sur des agents de sous-noeud. Bien que vous puissiez affecter des seuils à des groupes de ressources système basés sur des agents de sous-noeud, les événements ne s'affichent pas dans le Tableau de bord d'Application Performance. Les seuils sont affectés aux groupes de ressources système sur la base des agents de sous-noeud pour l'acheminement des événements. Les groupes de ressources système basés sur des agents de sous-noeud sont décrits comme suit dans le gestionnaire de groupes de ressources : 'les membres de ce groupe ne peuvent pas être ajoutés dans une application et les événements ne s'affichent pas dans la console Performance Management'. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 995.

Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit d'affichage pour un groupe de ressources système :

Tableau 208. Droits d'affichage pour un groupe de ressources système

Action	Droits disponibles
Afficher le groupe de ressources système dans le gestionnaire de groupes de ressources.	✓
Afficher des ressources qui font partie du groupe de ressources système dans la fenêtre Ajouter une application.	✓
Affecter des seuils au groupe de ressources système dans l'éditeur de seuils.	✓
Ajouter des ressources dans le groupe de ressources système.	—
Supprimer des ressources du groupe de ressources système.	—

Utilisation des rôles, des utilisateurs et des droits

La page Contrôle d'accès basé sur les rôles permet d'utiliser les rôles, les utilisateurs et les droits.

Procédure

- Pour filtrer la liste des rôles, des utilisateurs ou des groupes d'utilisateurs répertoriés dans la page Contrôle d'accès basé sur les rôles, procédez comme suit :
  1. Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  2. Cliquez dans la zone de texte Filtre et entrez le texte partiel ou complet qui servira de filtre. A mesure que vous tapez, les lignes qui ne contiennent pas ce que vous avez tapé dans la zone de filtre sont supprimées de la table.
  3. Pour supprimer le filtre rapide, supprimez la valeur ou cliquez sur «x».
  4. Pour appliquer le filtre, cliquez sur .
- Pour créer un rôle personnalisé, procédez comme suit :
  1. Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  2. Dans l'onglet **Rôles**, cliquez sur . La page **Editeur de rôle** s'affiche.
  3. Dans l'onglet **Affecter des utilisateurs à des rôles**, sélectionnez l'onglet **Groupes d'utilisateurs** ou l'onglet **Utilisateurs individuels**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à ajouter au rôle.
  4. Dans l'onglet **Affecter des droits à des rôles**, sélectionnez l'onglet **Droits d'accès de la configuration système** ou l'onglet **Droits d'accès aux ressources**, puis sélectionnez les droits à affecter au rôle.

5. Cliquez sur **Sauvegarder**.

- Pour éditer un rôle par défaut ou personnalisé existant, procédez comme suit :
  1. Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  2. Dans l'onglet **Rôles**, cliquez sur . La page **Editeur de rôle** s'affiche.
  3. Dans l'onglet **Affecter des utilisateurs à des rôles**, cliquez sur l'onglet **Groupes d'utilisateurs** ou l'onglet **Utilisateurs individuels**, puis sélectionnez les utilisateurs ou les groupes d'utilisateurs à ajouter au rôle.
  4. Dans l'onglet **Affecter des droits à des rôles**, sélectionnez l'onglet **Droits d'accès à la configuration système** ou l'onglet **Droits d'accès aux ressources**, puis sélectionnez les droits à affecter au rôle.
  5. Cliquez sur **Sauvegarder**.
- Pour supprimer un rôle, procédez comme suit :
  1. Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  2. Dans l'onglet **Rôles**, sélectionnez le rôle à supprimer, puis cliquez sur . Un message de confirmation s'affiche. Cliquez sur **OK**.

  Remarque : Lorsque vous supprimez un rôle, les utilisateurs membres de ce rôle ne sont pas supprimés. Ils restent disponibles dans l'onglet **Utilisateurs individuels** et peuvent être affectés à un autre rôle par l'administrateur des rôles.
- Pour éditer les droit d'accès d'un utilisateur individuel ou d'un groupe d'utilisateurs, procédez comme suit :
  1. Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  2. Dans l'onglet **Utilisateur individuel** ou **Groupes d'utilisateurs**, sélectionnez l'utilisateur ou le groupe d'utilisateurs à éditer, puis cliquez sur . La page **Editeur d'utilisateur individuel** s'ouvre.
  3. Sélectionnez le ou les rôles à affecter à l'utilisateur.
  4. Cliquez sur **Sauvegarder**.
- Pour créer un fichier csv qui récapitule les droits d'un utilisateur individuel ou d'un groupe d'utilisateurs, procédez comme suit :
  1. Dans l'onglet **Utilisateur individuel** ou **Groupes d'utilisateurs**, sélectionnez l'utilisateur ou le groupe d'utilisateurs requis, puis cliquez sur . La page **Editeur d'utilisateur individuel** ou **Editeur de groupe d'utilisateurs** s'ouvre.
  2. Cliquez sur **Récapitulatif de l'exportation**.
  3. Sélectionnez **Sauvegarder**, puis cliquez sur **OK**.

  Un fichier CSV récapitulant les droits de l'utilisateur ou du groupe d'utilisateurs est sauvegardé dans l'emplacement spécifié.

Résultats

L'affectation des rôles et des droits est appliqué dès que vous avez cliqué sur **Sauvegarder**.

Configuration de la consignation d'audit pour l'activité de contrôle d'accès basé sur les rôles

La fonction de consignation d'audit de Cloud APM consigne les événements importants liés à l'activité de contrôle d'accès basé sur les rôles. La sortie de cette fonction permet de déterminer les informations suivantes :

- Qui (utilisateur, service ou processus) a lancé l'action ?
- Quelle activité s'est produite et quel en a été le résultat ?
- Quand l'activité a-t-elle eu lieu ?
- Où l'activité a-t-elle été observée ?

- Quelle ressource l'activité a-t-elle ciblé ?
- Où l'activité a-t-elle été lancée ?
- Où était la cible de l'activité ?

Remarque : La fonction de consignation d'audit ne capture pas les événements liés à l'authentification des utilisateurs, par exemple, elle ne capture rien si un utilisateur est créé ou supprimé, mais elle capture les événements si un utilisateur est ajouté à un rôle ou supprimé d'un rôle. Toutes les activités de la page Contrôle d'accès basé sur les rôles réalisées par un administrateur de rôles sont capturées.

Chaque événement de journal d'audit est écrit comme unique ligne dans le fichier journal d'audit. Un événement de journal d'audit possède la structure générale suivante :

```
<AuditEvent ...>
<Who ... />
<What .../>
<When .../>
<OnWhat .../>
<Where .../>
<WhereFrom .../>
<WhereTo .../>
</AuditEvent>
<AuditEvent ...>
```

L'outil de collecte d'identification de problème permet de collecter les journaux requis et d'autres informations relatives à l'identification et la résolution des problèmes. La sortie de cet outil est demandée par le support IBM si vous ouvrez un ticket de demande de service. Les fichiers des journaux d'audit et des journaux de trace sont collectés lorsque vous exécutez l'outil de collecte d'identification de problème. Pour plus d'informations, voir Chapitre 16, «Traitement des incidents et support», à la page 1189.

Configuration de la consignation d'audit

L'emplacement des fichiers journaux d'audit, le nombre de fichiers journaux conservés et la taille maximale des fichiers journaux sont contrôlés dans le fichier `w7auditconfig.properties` qui se trouve dans le répertoire *rép_install*`/wlp/usr/servers/server1/cscs/conf`.

Procédure

1. Ouvrez le fichier `w7auditconfig.properties` qui se trouve dans le répertoire *rép_install*`/wlp/usr/servers/server1/cscs/conf`.

   Où
   rép_install est le répertoire où le serveur Cloud APM est installé
2. Pour spécifier la taille maximale en octets d'un fichier journal d'audit unique, éditez la propriété suivante :

   ```
   AUDIT_LIMIT_BYTES=2097152
   ```

   La valeur par défaut est 2097152. La fonction de consignation d'audit prend en charge l'approche des fichiers journaux générationnels. Des fichiers journaux d'audit sont créés lorsqu'un fichier journal d'audit atteint la taille maximale, telle qu'elle est spécifiée dans la propriété `AUDIT_LIMIT_BYTES`.
3. Pour spécifier le nombre maximal de fichiers journaux d'audit uniques créés avant bouclage, éditez la propriété suivante :

   ```
   AUDIT_COUNT=10
   ```

   La valeur par défaut est 10.
4. Pour spécifier le répertoire dans lequel les fichiers journaux d'audit sont sauvegardés, éditez la propriété suivante :

   ```
   AUDIT_PATH=rép_install/wlp/usr/servers/server1/logs
   ```

Où
rép_install est le répertoire où le serveur Cloud APM est installé

Les fichiers des journaux d'audit utilisent la convention de dénomination suivante :

```
nomhôte_horodatage.w7_audit.log
```

Où
nomhôte représente le nom d'hôte abrégé de la machine sur laquelle l'audit est consigné
horodatage représente l'horodatage de création du fichier du journal d'audit

Configuration de la consignation de trace pour la consignation d'audit

Si une consignation d'audit plus détaillée est requise, activez l'attribut `traceSpecification` dans le fichier *rép_install*`/wlp/usr/servers/server1/server.xml`.

Procédure

1. Ouvrez le fichier *rép_install*`/wlp/usr/servers/server1/server.xml`.

   Où
   rép_install est le répertoire où le serveur Cloud APM est installé
2. Copiez l'élément xml traceSpecification de `server.xml` dans `user-exit.xml`. `user-exit.xml` est un fichier de remplacement pour `server.xml`. Modifiez `user-exit.xml` comme suit :

   ```
   com.ibm.smai.cscs.service=finest
   com.ibm.apm.cscs.audit.impl=finest
   com.ibm.tivoli.audit.w7.*=finest
   ```

   Vérifiez que chaque option est délimitée par deux-points. Supprimez l'élément XML traceSpecification du fichier `server.xml`.

Résultats

Les instructions de trace sont enregistrées dans le fichier *rép_install*`/wlp/usr/servers/server1/logs/trace*.log`, où *rép_install* désigne le répertoire dans lequel le serveur Cloud APM est installé.

Configuration des certificats pour la console Cloud APM

Configurez des certificats personnalisés à l'aide d'une autorité de certification racine privée ou tierce pour activer la communication entre le serveur Cloud APM et la console Cloud APM.

Les certificats par défaut pour la console Cloud APM sont des certificats autosignés créés lors de l'installation du serveur Cloud APM. Les certificats n'étant pas signés par une autorité de certification de confiance, les utilisateurs de la console Cloud APM voient les erreurs de certificat dans leurs navigateurs lorsqu'ils accèdent à la console. Deux options sont possibles pour la suppression des messages d'erreur de certificat :

- Utilisez le serveur Cloud APM pour créer un certificat d'autorité de certification racine privée et utilisez-le pour signer les certificats utilisés par les processus de serveur Cloud APM. Fournissez ensuite le fichier d'autorité de certification racine privée aux utilisateurs de la console Cloud APM afin qu'ils l'importent dans la liste des autorités de certification racines de confiance dans leurs navigateurs.
- Utilisez une autorité de certification racine tierce (telle que GeoTrust ou une autorité de certification dans votre société) pour signer les certificats utilisés par les processus de serveur Cloud APM. Si l'autorité de certification racine tierce n'est pas déjà jugée comme étant sécurisée par les navigateurs des utilisateurs de la console Cloud APM, ils doivent importer le fichier d'autorité de certification racine dans la liste des certificats d'autorités de certification racines de confiance dans leurs navigateurs.

Configuration des certificats à l'aide d'une autorité de certification racine privée

Vous pouvez utiliser le serveur Cloud APM pour créer un fichier d'autorité de certification racine privée pour signer les certificats utilisés par les processus de serveur.

Les utilisateurs de votre console Cloud APM doivent alors importer le certificat d'autorité de certification racine privée dans la liste des autorités de certification racines de confiance dans leurs navigateurs afin que les certificats Cloud APM soient accrédités par leurs navigateurs.

Pourquoi et quand exécuter cette tâche

- Utilisez le répertoire `/opt/ibm` par défaut en tant que répertoire dans lequel vous avez installé le serveur Cloud APM ou utilisez le chemin que vous avez indiqué pour l'installation.
- Remplacez *nom_hôte_serveur_apm* par le nom d'hôte du serveur Cloud APM. Utilisez le nom d'hôte qualifié complet (tel que `myapmserver.ibm.com`) sauf si les utilisateurs de la console Cloud APM peuvent utiliser le nom d'hôte abrégé (tel que `myapmserver`). Par exemple, remplacez `Signer_CA_on_`*`nom_hôte_serveur_apm`* dans les étapes suivantes par `Signer_CA_on_myapmserver.ibm.com`.
- Remplacez *mot_de_passe* dans les étapes suivantes soit par `ROOTCAPASS`, qui est le mot de passe de l'autorité de certification racine, soit par `APMPASS`, qui est le mot de passe du magasin de clés de l'interface utilisateur du serveur Cloud APM.
- Remplacez *nom_de_ma_société* par le nom de votre société, IBM par exemple.
- Deux options sont disponibles pour l'algorithme de clé : RSA ou Elliptic Curve (EC). L'algorithme utilisé par l'autorité de certification pour signer ses certificats racine et intermédiaire doit correspondre à l'algorithme spécifié dans le paramètre **`-keyalg`**. La procédure suppose que l'algorithme RSA est utilisé. Si le certificat de l'autorité de certification racine a été signé à l'aide de l'algorithme Elliptic Curve, remplacez **`-keyalg RSA`** par **`-keyalg EC`** à chaque étape de cette procédure à laquelle un algorithme de clé est spécifié.
- Si vous copiez des commandes directement à partir du texte et que vous les collez sur la ligne de commande, copiez-les à partir de la version HTML de cette rubrique dans IBM Knowledge Center. La version PDF comporte des sauts de ligne destinés à accepter les limites de largeur de page qui ne doivent pas nécessairement être lus comme une nouvelle commande.

Procédure

1. Créez le certificat d'autorité de certification racine privée :

   ```
   export ROOTCAPASS="mot_de_passe"
   ```

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -genrootca -workdir "/opt/ibm/ccm
   /uikeyfiles" -keyalg RSA -hostname Root_CA_on_nom_hôte_serveur_apm -dname
    "O=nom de ma société" -label "Root_CA_for_APM_UI"
   ```

2. Générez la demande de signature de certificat (CSR) pour l'autorité de certification signataire :

   ```
   export APMPASS="mot_de_passe"
   ```

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -gencsr
   -workdir /opt/ibm/ccm/uikeyfiles -keyalg RSA -hostname Signer_CA_on_nom_hôte_serveur_apm
    -dname "O=nom_de_ma_société" -label "Signer_CA_for_APM_UI"
   ```

3. Importez le certificat de l'autorité de certification racine dans la base de données de clés de l'autorité de certification signataire :

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -addkeytodb
    -destkdb /opt/ibm/ccm/uikeyfiles/Signer_CA_on_nom_hôte_serveur_apm/keyfiles/keyfile.kdb -
   importfile /opt/ibm/ccm/uikeyfiles/apmCA/exports/apmCA.cer
    -label "Root_CA_for_APM_UI"
   ```

4. Signez le certificat de l'autorité de certification signataire :

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -signcsr -keyalg RSA
    -rootcakdb /opt/ibm/ccm/uikeyfiles/apmCA/keyfiles/keyfile.kdb
    -rootcalabel "Root_CA_for_APM_UI" -csrfile /opt/ibm/ccm/uikeyfiles
   /Signer_CA_on_nom_hôte_serveur_apm/exports/Signer_CA_on_apm_server_hostname.arm
    -ca true
   ```

5. Générez la demande de signature de certificat (CSR) pour le certificat du serveur Cloud APM :

```
/opt/ibm/ccm/create_security_artifacts.sh -gencsr -workdir /opt/ibm/
ccm/uikeyfiles -keyalg RSA -hostname nom_hôte_serveur_apm
 -dname "O=nom de ma société" -san_name
 nom_hôte_serveur_apm -label "defaultKeyStore"
```

Vous devez spécifier `defaultKeyStore` comme libellé pour ne pas avoir à modifier l'alias du magasin de clés dans le fichier `server.xml` pour les processus apmui, server1, uviews et oidc.

6. Ajoutez le certificat de l'autorité de certification racine à la base de données de clés pour le certificat du serveur Cloud APM :

```
/opt/ibm/ccm/create_security_artifacts.sh -addkeytodb
 -destkdb /opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.kdb
 -importfile /opt/ibm/ccm/uikeyfiles/apmCA/exports/apmCA.cer
 -label "Root_CA_for_APM_UI"
```

7. Ajoutez le certificat de l'autorité de certification signataire à la base de données de clés pour le certificat du serveur Cloud APM :

```
/opt/ibm/ccm/create_security_artifacts.sh -addkeytodb
 -destkdb /opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.kdb
 -importfile /opt/ibm/ccm/uikeyfiles/Signer_CA_on_nom_hôte_serveur_apm/exports/
Signer_CA_on_nom_hôte_serveur_apm.cer -label "Signer_CA_for_APM_UI"
```

8. Signez le certificat du serveur Cloud APM avec l'autorité de certification signataire :

```
/opt/ibm/ccm/create_security_artifacts.sh -signcsr -keyalg RSA
 -rootcakdb /opt/ibm/ccm/uikeyfiles/Signer_CA_on_nom_hôte_serveur_apm/keyfiles/keyfile.kdb -
rootcalabel "Signer_CA_for_APM_UI" -csrfile /opt/ibm/ccm
/uikeyfiles/nom_hôte_serveur_apm/exports/nom_hôte_serveur_apm.arm
```

9. Convertissez le certificat signé du serveur Cloud APM au format JKS :

```
/opt/ibm/ccm/create_security_artifacts.sh -kdb2jks -sourcekdb /opt/ibm
/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.kdb
```

10. Pour supprimer les mots de passe de l'environnement de ligne de commande, entrez ces commandes :

```
export -n APMPASS
```

```
export -n ROOTCAPASS
```

11. Copiez le certificat signé du serveur Cloud APM à l'emplacement partagé pour les processus apmui, server1, uviews et oidc :

```
cp /opt/ibm/wlp/usr/shared/resources/security/key.jks /opt/ibm/wlp/usr/shared
/resources/security/key.jks.sav
```

```
cp /opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.jks /opt/
ibm/wlp/usr/shared/resources/security/key.jks
```

12. Codez la valeur du mot de passe `APMPASS` à partir de l'étape 3 à l'aide de l'outil Liberty securityUtility et du chiffrement AES :

```
/opt/ibm/wlp/bin/securityUtility encode --encoding=aes mot_de_passe
```

13. Mettez à jour le mot de passe du magasin de clés dans le fichier `/opt/ibm/wlp/usr/shared/config/serverVariables.xml` :
    a. Recherchez la ligne contenant **`key.store.password`**.
    b. Remplacez la valeur par la sortie de l'étape précédente (étape 12).
14. Mettez à jour l'entrée oidc dans le magasin de clés de confiance partagé avec le nouveau certificat signé du serveur Cloud APM :

```
cp /opt/ibm/wlp/usr/shared/resources/security/trust.jks /opt/ibm/wlp/usr/
shared/resources/security/trust.jks.sav
```

```
/opt/ibm/java/jre/bin/keytool -delete -alias oidc -keystore /opt/ibm/wlp/
usr/shared/resources/security/trust.jks -storepass 'ccmR0cKs!'
```

```
/opt/ibm/java/jre/bin/keytool -importcert -alias oidc -file /opt/ibm/ccm/uikeyfiles
/nom_hôte_serveur_apm/exports/nom_hôte_serveur_apm.cer -noprompt -keystore /opt/ibm/wlp/usr/shared
/resources/security/trust.jks -storepass 'ccmR0cKs!'
```

où *ccmR0cKs!* est le mot de passe du magasin de clés de confiance par défaut. Si vous souhaitez utiliser un mot de passe différent, suivez la procédure décrite dans «Modification du mot de passe du magasin de clés de confiance partagé», à la page 1036 et utilisez le nouveau mot de passe dans cette étape.

15. Ajoutez le certificat de l'autorité de certification racine au magasin de clés de confiance Java :
    a. Exécutez la commande suivante :
    ```
    /opt/ibm/java/bin/keytool -importcert
     -file /opt/ibm/ccm/uikeyfiles/apmCA/exports/apmCA.cer
     -keystore /opt/ibm/java/jre/lib/security/cacerts -alias Root_CA_for_APM_UI
    ```
    b. Lorsque vous y êtes invité, entrez le mot de passe du magasin de clés :
    ```
    changeit
    ```
    c. Lorsque vous êtes invité à indiquer ce certificat, entrez `yes`.
16. Redémarrez les processus du serveur Cloud APM :
    ```
    apm restart_all
    ```
17. Envoyez les fichiers `/opt/ibm/ccm/uikeyfiles/apmCA/exports/apmCA.cer` et `/opt/ibm/ccm/uikeyfiles/Signer_CA_on_`*`nom_hôte_serveur_apm`*`/exports/Signer_CA_on_`*`apm_server_hostname`*`.cer` aux utilisateurs de la console Cloud APM.
    - Ces derniers doivent importer le fichier `apmCA.cer` dans la liste des certificats racine de confiance de leur navigateur, puis indiquer à celui-ci qu'il doit faire confiance au certificat dans le cadre de l'identification des sites Web.
    - Ils doivent également importer le fichier `Signer_CA_on_`*`nom_hôte_serveur_apm`*`.cer` dans la liste des autorités de certification intermédiaire, dans la mesure où elle existe, puis indiquer au navigateur qu'il doit faire confiance au certificat dans le cadre de l'identification des sites Web. Si le navigateur ne contient aucune liste des autorités de certification intermédiaire, les utilisateurs doivent alors importer le certificat dans la liste des certificats racine.
    - Les étapes d'importation de l'autorité de certification racine dépendent du navigateur et de la version du navigateur. Pour plus d'informations, voir la documentation de votre navigateur Web.

Résultats

Après avoir importé le certificat racine privé et le certificat de signataire, les utilisateurs de la console Cloud APM ne voient plus les erreurs de certificat indiquant que les certificats du serveur Cloud APM ne sont pas signés par une autorité de certification racine de confiance.

Configuration des certificats à l'aide d'une autorité de certification racine tierce

Vous pouvez créer un certificat personnalisé non signé par vos soins, mais généré par une autorité de certification tierce.

Pourquoi et quand exécuter cette tâche

- Utilisez le répertoire `/opt/ibm` par défaut en tant que répertoire dans lequel vous avez installé le serveur Cloud APM ou utilisez le chemin que vous avez indiqué pour l'installation.
- Remplacez *nom_hôte_serveur_apm* par le nom d'hôte du serveur Cloud APM. Utilisez le nom d'hôte qualifié complet (tel que `myapmserver.ibm.com`) sauf si les utilisateurs de la console Cloud APM peuvent utiliser le nom d'hôte abrégé (tel que `myapmserver`). Par exemple, remplacez `Signer_CA_on_`*`nom_hôte_serveur_apm`* dans les étapes suivantes par `Signer_CA_on_myapmserver.ibm.com`.
- Remplacez *mot_de_passe* dans les étapes suivantes soit par `ROOTCAPASS`, qui est le mot de passe de l'autorité de certification racine, soit par `APMPASS`, qui est le mot de passe du magasin de clés de l'interface utilisateur du serveur Cloud APM.
- Remplacez *nom_de_ma_société* par le nom de votre société, IBM par exemple.
- Deux options sont disponibles pour l'algorithme de clé : RSA ou Elliptic Curve (EC). L'algorithme utilisé par l'autorité de certification pour signer ses certificats racine et intermédiaire doit correspondre à l'algorithme spécifié dans le paramètre **`-keyalg`**. La procédure suppose que l'algorithme RSA est

utilisé. Si le certificat de l'autorité de certification racine a été signé à l'aide de l'algorithme Elliptic Curve, remplacez **-keyalg RSA** par **-keyalg EC** à chaque étape de cette procédure à laquelle un algorithme de clé est spécifié.

- Si vous copiez des commandes directement à partir du texte et que vous les collez sur la ligne de commande, copiez-les à partir de la version HTML de cette rubrique dans IBM Knowledge Center. La version PDF comporte des sauts de ligne destinés à accepter les limites de largeur de page qui ne doivent pas nécessairement être lus comme une nouvelle commande.

Procédure

1. Créez la demande de signature de certificat (CSR) :
   a. Ajoutez le mot de passe de votre magasin de clés à l'environnement :
      ```
      export APMPASS="mot_de_passe"
      ```
      où *mot_de_passe* est le mot de passe administrateur du serveur Cloud APM.
   b. Créez un répertoire `uikeyfiles` destiné à contenir les répertoires associés à votre demande de signature de certificat, sous `/opt/ibm/ccm`:
      ```
      mkdir /opt/ibm/ccm/uikeyfiles
      ```
      Ces fichiers sont inclus au cours des procédures de sauvegarde et de restauration du serveur Cloud APM.
   c. Exécutez le script suivant :
      ```
      ./create_security_artifacts.sh -gencsr -workdir /opt/ibm/ccm/uikeyfiles
      -keyalg RSA -hostname nom_hôte_serveur_apm -dname OU=ou,O=o,L=l,ST=st,C=c
      -label defaultKeyStore
      ```
      Vous devez spécifier `defaultKeyStore` comme libellé pour ne pas avoir à modifier l'alias du magasin de clés dans le fichier `server.xml` pour les processus apmui, server1, uviews et oidc.

   Une demande de signature de certificat est créée dans `/opt/ibm/ccm/uikeyfiles/`*nom_hôte_serveur_apm*`/exports/`*nom_hôte_serveur_apm*`.arm` que vous envoyez pour qu'elle soit signée par votre autorité de certification. Cette dernière renvoie votre nouveau certificat, le certificat d'émetteur et tout autre certificat dans la chaîne de confiance du certificat d'émetteur. Elle crée également un ensemble de fichiers dans `/opt/ibm/ccm/uikeyfiles/`*nom_hôte_serveur_apm*`/keyfiles` qui doit être mis à jour lorsque vous obtenez vos certificats de l'autorité de certification tierce et les importez dans `opt/ibm/ccm/uikeyfiles/`*nom_hôte_serveur_apm*`/keyfiles/keyfile.kdb`. Ces fichiers doivent être conservés et sont réutilisés dans les étapes qui suivent.

   Certaines versions plus récentes de Chrome exigent que les certificats importés spécifient un autre nom de l'objet DNS. Si votre autorité de certification n'ajoute pas l'autre nom d'objet automatiquement, vous pouvez l'ajouter à la demande de signature de certificat avec le paramètre **-san_name**. Si votre certificat est généré sans autre nom de l'objet DNS, les utilisateurs de Chrome doivent remplacer le message d'avertissement lorsqu'ils démarrent la console Cloud APM.

   Le paramètre **-gencsr** crée une clé privée qui se trouve actuellement dans le fichier `keyfile.rdb`. Cette dernière sera transférée ultérieurement dans le fichier `keyfile.kdb` lors de l'exécution de l'importation.
2. Une fois que vos certificats ont été renvoyés, ajoutez le certificat racine, les certificats intermédiaires et le certificat d'émetteur dans le fichier `keyfile.kdb` qui a été créé avec le paramètre **-gencsr** :
   a. Ajoutez le certificat racine de votre autorité de certification :
      ```
      /opt/ibm/ccm/create_security_artifacts.sh –addkeytodb -destkdb /opt/ibm/ccm/uikeyfiles
      /nom_hôte_serveur_apm/keyfiles/keyfile.kdb -
      importfile chemin_cert_racine_de_votre_autorité_certification
       -label libellé_racine_de_votre_autorité_certification
      ```
   b. Ajoutez le certificat intermédiaire de votre autorité de certification (si nécessaire) :
      ```
      /opt/ibm/ccm/create_security_artifacts.sh -addkeytodb -destkdb /opt/ibm/ccm
      /uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.kdb -importfile
       chemin_cert_intermédiaire_de_votre_autorité_certification -label libellé_intermédiaire_de_votre_autorité_certifica
      ```

Tous les fichiers de clés doivent également se trouver dans ce répertoire car ils sont utilisés par les étapes suivantes, même si vous spécifiez uniquement le chemin d'accès au fichier `keyfile.kdb`. Vous ajoutez cependant au préalable les certificats pour générer la chaîne de confiance.

3. Importez votre nouveau certificat et le certificat de signataire.

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -importcert
   -rootcacert chemin_cert_émetteur_autorité_certification -rootcalabel libellé_certificat_d'émetteur
   -destkdb /opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.kdb
   -importfile chemin_accès_nouveau_certificat_signé
   ```

   Cette commande est inhabituelle car elle utilise «rootcalabel» et «rootcacert» pour les noms de paramètre correspondant au certificat signataire. Les fichiers de magasin de clés dans `/opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles` sont maintenant modifiés et le fichier `keyfile.kdb` peut maintenant être converti au format jks.

4. Convertissez le fichier `keyfile.kdb` au format jks :

   ```
   /opt/ibm/ccm/create_security_artifacts.sh -kdb2jks –sourcekdb /opt/ibm/ccm/
   uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.kdb
   ```

   Deux fichiers sont créés : `/opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.jks` et `/opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.p12`. Le fichier `p12` n'est pas utilisé pour Cloud APM mais openssl prend en charge ce format de magasin de clés et il peut être validé à l'aide de `openssl pkcs12 -in /opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.p12`.

5. Pour supprimer le mot de passe de l'environnement de ligne de commande, entrez la commande suivante :

   ```
   export -n APMPASS
   ```

6. Copiez le nouveau magasin de clés à l'emplacement partagé pour les serveurs apmui, server1, uviews et oidc :

   a. Sauvegardez le magasin de clés d'origine :

      ```
      cp /opt/ibm/wlp/usr/shared/resources/security/key.jks /opt/ibm/wlp/usr/shared/resources
      /security/key.jks.sav
      ```

   b. Copiez le nouveau magasin de clés :

      ```
      cp /opt/ibm/ccm/uikeyfiles/nom_hôte_serveur_apm/keyfiles/keyfile.jks /opt/ibm/wlp/usr/shared
      /resources/security/key.jks
      ```

7. Exécutez l'outil Liberty securityUtility avec l'option AES pour coder le mot de passe de votre magasin de clés que vous avez ajouté à l'environnement dans APMPASS. Répondez à l'invite `Enter text:` avec votre mot de passe.

   ```
   /opt/ibm/wlp/bin/securityUtility encode --encoding=aes
   Enter text:
   Re-enter text:
   {aes}votre_mot_de_passe_codé
   ```

8. Mettez à jour le mot de passe du magasin de clés dans le fichier `/opt/ibm/wlp/usr/shared/config/serverVariables.xml` en recherchant la ligne contenant **`key.store.password`** et remplacez la valeur par la sortie de l'étape précédente (étape 7). Veillez à inclure `{aes}` avant votre mot de passe codé dans le fichier XML.

9. Mettez à jour l'entrée oidc dans le magasin de clés de confiance partagé avec votre certificat :

   a. Sauvegardez l'original :

      ```
      cp /opt/ibm/wlp/usr/shared/resources/security/trust.jks /opt/ibm/wlp/usr/shared/resources
      /security/trust.jks.orig
      ```

   b. Supprimez l'entrée oidc :

      ```
      /opt/ibm/java/bin/keytool -delete -alias oidc -keystore /opt/ibm/wlp/usr/shared/resources
      /security/trust.jks -storepass 'ccmR0cKs!'
      ```

où *ccmR0cKs!* est le mot de passe du magasin de clés de confiance par défaut. Si vous souhaitez utiliser un mot de passe différent, suivez la procédure décrite dans «Modification du mot de passe du magasin de clés de confiance partagé» et utilisez le nouveau mot de passe dans cette étape.

c. Ajoutez le nouveau certificat en tant qu'entrée oidc :

```
/opt/ibm/java/bin/keytool -importcert -alias oidc -file path_to_new_signed_cert
 -noprompt -keystore /opt/ibm/wlp/usr/shared/resources/security/trust.jks -storepass 'ccmR0cKs!'
```

où *ccmR0cKs!* est le mot de passe du magasin de clés de confiance par défaut. Si vous souhaitez utiliser un mot de passe différent, suivez la procédure décrite dans «Modification du mot de passe du magasin de clés de confiance partagé» et utilisez le nouveau mot de passe dans cette étape.

10. Si votre autorité de certification racine tierce n'est pas bien connue, ajoutez ce certificat au magasin de clés de confiance Java :

a. Exécutez la commande suivante :

```
/opt/ibm/java/bin/keytool -importcert -file chemin_certificat_autorité_certification_racine
 -keystore /opt/ibm/java/jre/lib/security/cacerts
 -alias certificat_autorité_certification_racine
```

b. Lorsque vous y êtes invité, entrez le mot de passe suivant :

```
changeit
```

c. Lorsque vous êtes invité à indiquer ce certificat, entrez `yes`.

11. Redémarrez les processus du serveur Cloud APM :

```
apm restart_all
```

12. Envoyez le fichier de certificat racine aux utilisateurs de la console Cloud APM.
    - Ces derniers doivent importer le certificat racine dans la liste des certificats racine de confiance de leur navigateur, puis indiquer à celui-ci qu'il doit faire confiance au certificat dans le cadre de l'identification des sites Web.
    - Certains navigateurs nécessitent également l'importation des certificats intermédiaires. Dans ce cas, les utilisateurs doivent importer le fichier de certificat intermédiaire dans la liste des autorités de certification intermédiaire, puis indiquer au navigateur qu'il doit faire confiance au certificat dans le cadre de l'identification des sites Web.
    - Les étapes d'importation de l'autorité de certification racine dépendent du navigateur et de la version du navigateur. Pour plus d'informations, voir la documentation de votre navigateur Web.

Modification du mot de passe du magasin de clés de confiance partagé

Le magasin de clés de confiance partagé est utilisé par les serveurs Liberty sélectionnés pour vérifier les accréditations. S'il y a lieu, vous pouvez modifier le mot de passe.

Avant de commencer

Remplacez `/opt/ibm` par le chemin d'installation que vous avez indiqué lors de l'installation du serveur Cloud APM.

Procédure

1. Vérifiez que vous connaissez le mot de passe en cours du magasin de clés de confiance partagé. Exécutez la commande suivante :

```
cd /opt/ibm/wlp/usr/shared/resources/security/
keytool -list -v -keystore trust.jks
```

A l'invite du système, entrez le mot de passe. Le mot de passe par défaut est :

```
ccmR0cKs!
```

La commande doit imprimer les alias de toutes les entrées du magasin de clés.

2. Arrêtez le serveur Cloud APM :

   ```
   apm stop_all
   ```

3. Modifiez le mot de passe du magasin de clés de confiance :

   ```
   cd /opt/ibm/wlp/usr/shared/resources/security/
   cp trust.jks trust.jks.sav
   keytool -storepasswd -keystore trust.jks
   ```

4. Codez le mot de passe à l'aide de l'outil Liberty securityUtility et du chiffrement AES :

   ```
   /opt/ibm/wlp/bin/securityUtility encode --encoding=aes
   ```

5. Mettez à jour la configuration du serveur Cloud APM :

   ```
   cd /opt/ibm/wlp/usr/shared/config/
   cp serverVariables.xml serverVariables.xml.sav
   ```

   Mettez à jour la valeur de la variable `trust.store.password` dans le fichier `serverVariables.xml`. Utilisez pour ce faire la valeur déterminée à l'étape 4, par exemple :

   ```
   <variable name="trust.store.password" value="{aes}AKPjaLK2Ng7Epa+PX41P0yWfbfyu98/g0FhhGDx/
   wpK/" />
   ```

6. Démarrez le serveur Cloud APM :

   ```
   apm start_all
   ```

Accès et utilisation de l'API Role-Based Access Control Service

Utilisez l'API Role-Based Access Control Service pour gérer le cycle de vie des stratégies de contrôle d'accès basé sur les rôles à partir de la ligne de commande.

Pourquoi et quand exécuter cette tâche

Effectuez des tâches d'accès basé sur les rôles telles que la création, l'affichage, la mise à jour et la suppression de rôles. Ajoutez et supprimez un ensemble d'utilisateurs ou de groupes d'utilisateurs à partir d'un rôle donné. Accordez des droits à un rôle donné. Affichez une liste des rôles, utilisateurs, groupes d'utilisateurs et droits qui sont définis dans le système.

Vous pouvez créer des scripts d'automatisation de tâches telles que la définition de nouveaux rôles et l'affectation d'utilisateurs, de groupes d'utilisateurs et de droits à ces rôles.

Dans cette tâche, vous pouvez utiliser des jetons d'accès ou une autorisation de base dans la commande curl :

Jetons d'accès

Utilisez le protocole OIDC (OpenID Connect) pour obtenir un jeton d'accès du serveur OIDC sur le serveur Cloud APM. Le jeton d'accès vous permet d'accéder à l'API pour exécuter des opérations jusqu'à ce que le jeton expire après 30 minutes.

Autorisation de base

Utilisez un outil base64 pour coder l'ID utilisateur et le mot de passe de votre console Cloud APM en une chaîne base64. Le format de la chaîne en entrée est *`IDutilisateur:mdp`*. Par exemple : `apmadmin:apmpass`. La sortie est une chaîne se présentant comme suit : `YXBtYWRtaW46YXBtcGFzcw==!`.

Utilisez la chaîne `base64_encoded_string` dans l'en-tête d'autorisation de chacune des demandes, comme illustré dans les exemples de commande curl.

Notez que l'ID utilisateur de la console Cloud APM doit être ajouté à un rôle disposant des droits appropriés.

La désactivation de l'authentification OIDC, qui est nécessaire avant l'activation de la connexion unique (SSO) entre Cloud APM et d'autres produits IBM tels que Tivoli Common Reporting requérant LTPA pour

la connexion unique, n'affecte pas l'API. L'API RESTful continue d'utiliser le serveur OIDC interne de Cloud APM même si OIDC est désactivé pour la connexion unique entre la console Cloud APM et les interfaces utilisateur d'autres produits.

Procédure

1. Sur le système où le serveur Cloud APM est installé, ouvrez le fichier suivant, puis copiez l'ID client et le secret client :

   ```
   /opt/ibm/wlp/usr/shared/config/clientSecrets.xml
   ```

   L'exemple suivant montre le contenu du fichier :

   ```
   <server>
     <variable name="client.secret.apmui" value="{xor}J2oZKWQsHXVxeCJwBGsc
   fQ40d2N+cBUPZmltKRNz" />
     <variable name="client.id.apmui" value="rpapmui" />
   </server>
   ```

2. Utilisez un décodeur XOR pour obtenir la valeur réelle du mot de passe. Exemple : `x5Fv;sB*.'}/[4C"Qk(<!/JP962vL`

3. (Facultatif) Si vous prévoyez d'utiliser un jeton d'accès dans votre commande curl, pour obtenir un jeton d'accès, contactez le noeud final du jeton du serveur OIDC en utilisant les quatre paramètres requis : **`username`**, **`password`**, **`client_id`** et **`client_secret`**. Dans cet exemple de curl, le paramètre **`client_secret`** a la valeur «secret» :

   ```
   curl --tlsv1.2 -v -k -d «grant_type=password
   &client_id=rpapmui&client_secret=secret
   &username=apmadmin&password=apmpass&scope=openid»
   https://example.mycompany.com:8099/oidc/endpoint/OP/token
   ```

   Output:

   ```
   {"access_token":"jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8",
   "token_type":"Bearer","expires_in":1800,"scope":"openid",
   "refresh_token":"VsCWUhPHBRpidD2F1PVyZ2LNGMuQPTN837t3OoqZj71FcBfsGE"}
   ```

4. (Facultatif) Si vous prévoyez d'utiliser un jeton d'accès dans votre commande curl, extrayez la valeur **`access_token`**. Si vous examinez le résultat de l'exemple précédent, la valeur est `jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8`.

5. Entrez les demandes à l'API Role-Based Access Control Service à l'aide d'un jeton d'accès ou d'une autorisation de base.
   Exemple avec jeton d'accès :

   ```
   curl --tlsv1.2 -v -k --request GET
   --url 'https://myAPMServer.mycompany-domain.com:9443/1.0/authzn/users'
   --header 'authorization: Bearer  jnz4Ad0zpeCpYcUlUf7o4A40tz5trnIW9GutICG8'
   --header 'content-type: application/json'
   ```

   Exemple avec autorisation de base :

   ```
   curl --tlsv1.2 -v -k --request GET
   --url 'https://myAPMServer.mycompany-domain.com:9443/1.0/authzn/users'
   --header 'authorization: Basic YXBtYWRtaW46YXBtcGFzcw==!'
   --header 'content-type: application/json'
   ```

6. Pour plus d'informations sur les opérations API, voir la documentation associée dans l'Explorateur d'API. Pour des instructions sur l'accès à l'Explorateur d'API, voir Exploration des API.

   Remarque : Une partie de l'URL et certains des en-têtes présentés dans les exemples sont requis uniquement pour Cloud APM. Par exemple : https://api.ibm.com/perfmgmt/run, x-ibm-service-location, X-IBM-Client-Id, X-IBM-Client-Secret. Voir l'étape 5 pour des exemples de requête.

7. Vous devez inclure un en-tête de référenceur dans toutes les demandes POST, PUT et DELETE. La valeur de l'en-tête de référenceur est la suivante :

   ```
   -H 'Referer: https://serveur_apm:9443'
   ```

où *serveur_apm* est l'adresse IP ou le nom d'hôte complet de votre serveur Cloud APM.

Exemple

L'exemple suivant utilise la commande curl pour créer un rôle.

```
POST /1.0/authzn/roles
```

Remarque : Le corps de la requête POST doit contenir un objet JSON qui définit le rôle tel qu'indiqué par le paramètre **-d**.

```
curl -X POST \
  https://serveur_apm:9443/1.0/authzn/roles \
  -H 'Referer: https://serveur_apm:9443' \
  -H 'authorization: Bearer votre_jeton_d'accès' \
  -H 'content-type: application/json' \
  -d '{
    "description": "Description de votre rôle",
    "id": "/authzn/roles/ID_de_votre_rôle",
    "label": "Nom de votre rôle"
}'
```

Administration de vos agents

Votre installation IBM Cloud Application Performance Management dispose d'outils permettant de gérer vos agents de surveillance.

Certains de ces outils sont également utilisés pendant la configuration initiale de vos systèmes gérés : «Utilisation des commandes de l'agent», à la page 213, «Page Configuration d'agent», à la page 218 et «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 217.

Démarrage d'agents en tant qu'utilisateur non superutilisateur

Si vous souhaitez démarrer des agents avec des utilisateurs différents, créez un groupe commun sur le système et affectez chaque utilisateur en tant que membre de ce groupe.

Avant de commencer

Si vous avez installé et configuré votre agent avec le même utilisateur non superutilisateur et que vous voulez le démarrer avec le même utilisateur, aucune action particulière n'est requise. Si vous avez installé et configuré votre agent avec un utilisateur sélectionné et que vous voulez le démarrer avec un autre utilisateur, créez un groupe commun sur le système. Affectez tous les utilisateurs de gestion d'agent en tant que membres de ce groupe commun. Transférez la propriété de tous les répertoires et fichiers d'agent à ce groupe.

Pourquoi et quand exécuter cette tâche

Un script de démarrage automatique est généré par une installation, une mise à niveau ou une configuration. Ce script, (nommé `ITMAgentsN` ou `rc.itmN` suivant le système d'exploitation UNIX), contient une entrée pour chaque application dans une installation particulière. Par défaut, tous les agents sont démarrés avec les droits d'accès de superutilisateur. Pour mettre à jour les scripts de démarrage du système et démarrer les agents en tant qu'utilisateur non superutilisateur, vous devez éditer le fichier `rép_install/config/kcirunas.cfg`, qui contient un sur-ensemble de la syntaxe XML. Chaque section **`productCode`** dans le fichier `kcirunas.cfg` est désactivée par défaut. Activez une section **`productCode`** pour votre agent en supprimant l'indicateur de commentaire dans **`!productCode`**. Les sections mises en commentaire ou désactivées sont ignorées. Les sections non mises en commentaire ou activées pour des applications qui ne sont pas installées sont ignorées.

Procédure

1. Installez vos agents de surveillance sous Linux ou AIX, comme indiqué dans «Installation d'agents», à la page 167 sur des systèmes AIX ou dans «Installation d'agents», à la page 175 sur des systèmes Linux.
2. Facultatif : Au besoin, configurez vos agents de surveillance sous Linux ou AIX (voir Chapitre 10, «Configuration de votre environnement», à la page 201).
3. Exécutez le script `./secure.sh` avec le nom de groupe de l'utilisateur non superutilisateur afin de sécuriser les fichiers et définissez la propriété de groupe de fichiers sur les fichiers. Par exemple : **`./secure.sh -g db2iadm1`**
4. Pour mettre à jour les scripts de démarrage du système, procédez comme suit :
   a. Mettez à jour le fichier `rép_install/config/kcirunas.cfg`. Activez les sections **`productCode`** pour vos agents. Pour les agents qui ne requièrent pas une valeur d'instance, indiquez le code_produit, l'instance et l'utilisateur, où *code_produit* correspond au code à deux lettres spécifié dans tableau 27, à la page 213. Pour les agents qui requièrent une valeur d'instance, tels que l'agent de surveillance Db2 (code produit : ud), indiquez le code_produit, l'instance, l'utilisateur et le nom. Par exemple :

```
<productCode>ud</productCode>
<instance>
<name>db2inst1</name>
<user>db2inst1</user>
</instance>
<instance>
<name>db2inst2</name>
<user>root</user>
</instance>
```

   b. Exécutez le script suivant avec les droits d'accès de superutilisateur ou d'utilisateur sudo : *`rép_install`*`/bin/UpdateAutoRun.sh`

Que faire ensuite

Pour plus d'informations sur le script **`./secure.sh`**, voir Securing the agent installation files.

Utilisez le même ID utilisateur pour l'installation et les mises à niveau des agents.

Gestion des valeurs de conservation des données d'historique

Vous pouvez modifier le nombre de jours pendant lesquels les échantillons de données de surveillance des ressources sont conservés dans la base de données du serveur Cloud APM, de la valeur par défaut de huit jours aux valeurs recommandées qui ont été établies par les développeurs de l'agent et du collecteur de données. Vous pouvez également personnaliser la conservation des données pour des jeux de données individuels de surveillance des ressources dans chaque agent ou collecteur de données, entre 2 jours (valeur minimale) et 32 jours (valeur maximale). La durée de conservation des données de suivi des transactions par l'Agent de surveillance des temps de réponse ou les agents middleware et les données de transactions synthétiques ne peut pas être modifiée.

Pourquoi et quand exécuter cette tâche

Après avoir redéfini la durée maximale de conservation des données sur une valeur supérieure à 8 jours pour les données de surveillance des ressources, vous pourrez visualiser les données comprises dans la durée de conservation maximale dans les onglets suivants de la console Cloud APM :

- Pour les graphiques à courbes du tableau de bord qui représentent un intervalle égal aux 4 dernières heures dans l'onglet Présentation des statuts, vous pouvez comparer les valeurs de l'intervalle du jour avec le même intervalle d'un autre jour jusqu'à la durée maximale de conservation. Par exemple, comparez l'intervalle du jour égal aux 4 dernières heures avec le même intervalle d'un autre jour, jusqu'à 32 jours plut tôt. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1138.

- Pour les vues personnalisées, vous pouvez afficher les données d'un intervalle pour n'importe quel jour compris dans la durée de conservation maximale ; par exemple, vous pouvez afficher un intervalle de 4 heures pour n'importe quel jour, ces 32 derniers jours. Pour plus d'informations, voir «Affichage de pages personnalisées», à la page 1167.

Remarque :

- Vous ne pouvez pas afficher de données datant de plus d'une semaine dans l'onglet Détails d'attribut, même si vous redéfinissez la durée de conservation maximale sur une valeur supérieure à 8 jours.
- Après avoir modifié la durée de conservation maximale, dans les onglets Présentation des statuts et Vues personnalisées, vous pouvez sélectionner un jour compris dans la durée de conservation maximale que vous avez définie. Par exemple, si vous configurez les valeurs recommandées, la console Cloud APM vous permet de sélectionner un jour compris dans les 32 derniers jours. Les valeurs recommandées ne permettent cependant pas de conserver 32 jours de données pour tous les ensembles de données. Les graphiques à courbes ou les vues personnalisées des ensembles de données qui possèdent une durée de conservation de 8 jours affichent donc des données uniquement si vous sélectionnez un jour de la semaine passée.
- Après avoir modifié la durée de conservation, le serveur Cloud APM commence à conserver les données pour le nombre de jours configuré et les données plus anciennes ne sont pas aussitôt disponibles. Par exemple, si vous activez la conservation aujourd'hui avec les valeurs recommandées, les données datant de ces 32 derniers jours ne peuvent pas s'afficher dans la console Cloud APM jusqu'à au moins 3 semaines à partir de la date du jour.
- Les données d'historique des transactions synthétiques et du suivi des transactions sont sauvegardées dans la base de données DATAMART. Les paramètres de conservation des données ne peuvent pas être modifiés pour les données de la base de données DATAMART. Pour afficher les données d'historique des transactions synthétiques ou des données de transaction de l'Agent de surveillance des temps de réponse, vous devez installer Tivoli Common Reporting et les rapports Cloud APM. Pour plus d'informations, voir «Intégration à Tivoli Common Reporting», à la page 917 et «Rapports», à la page 1172.

La base de données d'historique Db2 du serveur Cloud APM, WAREHOUS, conserve généralement 8 jours d'échantillons de données provenant des agents et des collecteurs de données IBM Cloud APM. Le nombre exact pour chaque jeu de données est publié dans l'aide sur les attributs de l'agent ou du collecteur de données, ainsi que dans le PDF de référence (voir Chapitre 2, «Documentation au format PDF», à la page 29).

Le serveur Cloud APM comporte un script `get_metrics_retention.sh` que vous pouvez exécuter pour afficher le nombre de jours pendant lesquels les échantillons de données sont conservés pour les jeux de données dans chaque agent de surveillance et collecteur de données, et un script `set_metrics_retention.sh` permettant d'ajuster ces valeurs dans le but d'adopter les valeurs recommandées (best practices) ou les modifications que vous spécifiez. Pour obtenir la description complète des paramètres pris en charge par les scripts de conservation des données d'historique, voir «Scripts de conservation des données d'historique», à la page 1043.

La procédure comporte des étapes pour 3 scénarios types : définissez la conservation des données aux valeurs recommandées (best practices), rétablissez la conservation à sa valeur par défaut de 8 jours, et appliquez les paramètres de conservation des données après avoir généré un fichier avec les paramètres de conservation des données d'historique actuels et modifié les valeurs.

Les scripts nécessitent le mot de passe de Db2_server_instance_user *db2apm*, tel que db2Usrpasswd@08 (voir Utilisateurs et mots de passe par défaut).

Procédure

Sur le système où est installé le serveur Cloud APM, accédez au répertoire `/opt/ibm/ccm` ou à celui que vous avez indiqué au cours de l'installation du serveur et exécutez l'une des étapes suivantes :

- Remplacez les paramètres de conservation des données par les valeurs recommandées (best practices) :
  `./set_metrics_retention.sh -pw db2_instance_user -retention BEST_PRACTICES`

  Après avoir entré y en réponse à l'invite, `Voulez-vous continuer ? (y/n)`, les paramètres de conservation des données sont modifiés pour être remplacés par les valeurs recommandées dans la base de données d'historique Db2.
- Rétablissez les valeurs par défaut des paramètres de conservation des données :
  `./set_metrics_retention.sh -pw db2_instance_user -retention 8DAYS`

  Après avoir entré y en réponse à l'invite, `Voulez-vous continuer ? (y/n)`, les paramètres de conservation des données sont rétablis à leurs valeurs par défaut de 8 jours dans la base de données d'historique Db2.
- Personnalisez les valeurs de conservation des données pour des jeux de données spécifiques :
  1. Entrez la commande suivante pour générer le fichier de configuration d'historique :
     `./get_metrics_retention.sh -pw db2_instance_user -retention CURRENT`

     Après avoir entré y en réponse à l'invite, `Voulez-vous continuer ? (y/n)`, les valeurs de conservation des données de tous les agents et collecteurs de données Cloud APM sont lues à partir de la base de données d'historique Db2 et renvoyées en sortie dans `tmp/history_file.cfg`.
  2. Modifiez les paramètres de conservation des données pour des jeux de données spécifiques en éditant `/tmp/history_file.cfg` de 2 à 32 jours. Par exemple, voici le jeu de données E/S de disque de l'Agent Linux OS une fois la valeur de conservation des données remplacée par 22 jours : `KLZ,KLZ_Disk_IO,KLZDSKIO,Detailed,22,D`.
  3. Après avoir sauvegardé vos modifications dans le fichier `history_file.cfg`, entrez la commande suivante :
     `./set_metrics_retention.sh -pw db2_instance_user -history tmp/history_file.cfg`

     Une fois que vous avez entré y en réponse à l'invite, `Voulez-vous continuer ? (y/n)`, les modifications apportées aux valeurs de conservation des données sont appliquées à la base de données d'historique Db2.

Exemple

Voici la section d'agent Windows OS du fichier `history_file.cfg` une fois les valeurs recommandées (best practices) définies :

```
****** PRODUCT CODE: KNT ******

KNT,Knt_LFAProfiles,KNTLFAPFLS,Detailed,32,D
KNT,Knt_Log_File_Status,KNTLOGFST,Detailed,8,D
KNT,Knt_LogfileProfileEvents,KNTLOGPEVT,Detailed,8,D
KNT,NT_Computer_Information,NTCOMPINFO,Detailed,8,D
KNT,NT_IP_Address,NTIPADDR,Detailed,8,D
KNT,NT_Monitored_Logs_Report,NTLOGINFO,Detailed,32,D
KNT,NT_Memory_64,NTMEMORY,Detailed,32,D
KNT,NT_Network_Interface,NTNETWRKIN,Detailed,32,D
KNT,NT_Paging_File,NTPAGEFILE,Detailed,32,D
KNT,NT_Process_64,NTPROCESS,Detailed,32,D
KNT,NT_Processor,NTPROCSSR,Detailed,32,D
KNT,NT_Logical_Disk,WTLOGCLDSK,Detailed,32,D
KNT,NT_Objects,WTOBJECTS,Detailed,32,D
KNT,NT_Physical_Disk,WTPHYSDSK,Detailed,14,D
KNT,NT_System,WTSYSTEM,Detailed,32,D
```

Que faire ensuite

Si vous modifiez la durée de conservation maximale, vous devez vous déconnecter de la console Cloud APM et vous reconnecter. Vous pourrez ensuite sélectionner un jour compris dans la nouvelle durée de

conservation maximale, dans l'onglet Présentation des statuts ou Vues personnalisées.

Scripts de conservation des données d'historique

Examinez les paramètres que vous pouvez spécifier lors de l'exécution des scripts de conservation des données d'historique pour apporter des modifications concernant par exemple le chemin du fichier de configuration d'historique ou le nom du serveur Db2 distant.

get_metrics_retention.sh

Le script `get_metrics_retention.sh` crée un fichier de configuration d'historique que vous pouvez utiliser pour examiner les paramètres de conservation des données en cours ou les paramètres que vous prévoyez d'appliquer. Le fichier de configuration d'historique est requis si vous prévoyez de personnaliser les valeurs de conservation des données des jeux de données individuels pour les agents ou les collecteurs de données.

-db_inst *instance_base_de_données*
Si vous avez utilisé un nom d'instance de base de données Db2 différent du nom db2apm par défaut, utilisez ce paramètre pour spécifier le nom.

-db_name *nom_base_de_données*
Indiquez un autre nom pour la base de données d'historique Db2.

-db_port *port_base_de_données*
Spécifiez le port Db2 lorsqu'il est différent du port par défaut 50000.

-h *rép_install*
Spécifiez un répertoire différent du répertoire d'installation par défaut `/opt/ibm` du serveur Cloud APM.

-help
Permet d'afficher les paramètres `get_metrics_retention.sh`.

-history *fichier_config_historique*
Pour le fichier de configuration d'historique, spécifiez un chemin et un nom différents du chemin et nom par défaut `tmp/history_file.cfg`, tel que `/root/myfile.cfg`.

-logName *nom_journal*
Spécifiez un nom de fichier journal différent du fichier journal par défaut `get_metrics_retention.sh_AAAAMMJJHHMM.log`.

-logPath *chemin_journal*
Spécifiez un répertoire différent du répertoire par défaut `/tmp` pour stocker le fichier journal.

-pw *mdp_instance*
Il s'agit du mot de passe de l'utilisateur d'instance db2apm, tel que db2Usrpasswd@08. Si vous utilisez le paramètre **-db_inst** pour spécifier une instance différente de db2apm, utilisez le mot de passe pour cette instance. Pour le script `get_metrics_retention.sh`, le mot de passe de l'utilisateur d'instance Db2 est requis uniquement lorsque vous spécifiez `-retention CURRENT`.

-quiet *Y|N*
Le paramètre par défaut est `N`. Pour désactiver l'invite `Voulez-vous continuer ? (y/n)`, utilisez `-quiet Y`. Si vous appelez ce script à partir d'un autre script ou de manière automatique, vous pouvez souhaitez désactiver l'invite interactive. La sortie est visible dans le fichier `get_metrics_retention.sh_AAAAMMJJHHMM.log`.

-retention *BEST_PRACTICES|8DAYS|2DAYS|CURRENT*
Génère le fichier de configuration d'historique avec les valeurs recommandées (best practices), 8 jours, 2 jours ou les valeurs actuelles (current).

-server *nom_hôte_serveur_base_de_données*
Lorsque votre serveur Cloud APM se connecte à un serveur Db2 distant plutôt qu'au serveur Db2 local par défaut, spécifiez l'adresse IP ou le nom d'hôte qualifié complet du serveur Db2.

Exemples :

Cette commande entre le mot de passe de l'utilisateur par défaut db2apm et crée un fichier hist/history_file.cfg avec les paramètres en cours :

```
./get_metrics_retention.sh -pw db2Usrpasswd@08 -h /opt/ibm/ccm/hist
-retention CURRENT
```

Cette commande crée un fichier de configuration d'historique /root/my_config_file.txt avec les valeurs recommandées (best practices) :

```
./get_metrics_retention.sh -history /root/my_config_file.txt
-retention BEST_PRACTICES
```

set_metrics_retention.sh

Le script set_metrics_retention.sh crée un fichier de configuration d'historique qui permet de modifier les valeurs de conservation des données des jeux de données de l'agent et des collecteurs de données dans le but d'adopter les valeurs recommandées (best practices), les modifications que vous spécifiez ou de rétablir les valeurs de conservation des données par défaut de 8 jours.

-db_inst ***instance_base_de_données***
Si vous avez utilisé un nom d'instance de base de données Db2 différent du nom db2apm par défaut, utilisez ce paramètre pour spécifier le nom.

-db_name ***nom_base_de_données***
Indiquez un autre nom pour la base de données d'historique Db2.

-db_port ***port_base_de_données***
Spécifiez le port Db2 lorsqu'il est différent du port par défaut 5000.

-h ***rép_install***
Spécifiez un répertoire différent du répertoire d'installation par défaut /opt/ibm du serveur Cloud APM.

-help
Affichez les paramètres set_metrics_retention.sh.

-history ***fichier_config_historique***
Indiquez le nom du fichier de configuration d'historique que vous avez personnalisé et appliqué à la base de données d'historique Db2 (WAREHOUS).

-ksy ***chemin_base_ksy***
Indiquez le chemin de base de l'agent Summarization and Pruning permettant de gérer les partitions de base de données et d'élaguer les données de surveillance sur le serveur Db2. Le chemin par défaut est *rép_install*/sy.

-logName ***nom_journal***
Spécifiez un nom de fichier journal différent du fichier journal par défaut set_metrics_retention.sh_*AAAAMMJJHHMM*.log.

-logPath ***chemin_journal***
Spécifiez un répertoire différent du répertoire par défaut tmp pour stocker le fichier journal.

-override ***ON|OFF|RESET***
Par défaut, -override est défini sur **ON**, ce qui signifie que les paramètres que vous appliquez avec le script set_metrics_retention.sh à la base de données d'historique Db2 ne sont pas modifiés par les mises à jour de Cloud APM au cours des mises à niveau. A moins d'avoir inclus le paramètre -override OFF lors de l'exécution du script set_metrics_retention.sh ou lors de l'exécution précédente du script, les paramètres d'historique mis à jour sont sauvegardés dans une table WAREHOUSESUMPRUNE_OVERRIDE pour indiquer que ces valeurs seront prioritaires par rapport aux futures mises à niveau.

La définition de `-override OFF` signifie que les valeurs sont valides uniquement jusqu'à la mise à niveau suivante de Cloud APM. Ils seront remplacés par les valeurs de base de données d'historique Db2 par défaut (WAREHOUS).

La définition de `-override RESET` supprime les entrées de la table WAREHOUSESUMPRUNE_OVERRIDE.

-pw *mdp_instance*
Il s'agit du mot de passe de l'utilisateur d'instance db2apm, tel que db2Usrpasswd@08. Si vous utilisez le paramètre **-db_inst** pour spécifier une instance différente de db2apm, utilisez le mot de passe pour cette instance.

-quiet *Y|N*
Le paramètre par défaut est `N`. Pour désactiver l'invite `Voulez-vous continuer ? (y/n)`, utilisez `-quiet Y`. Si vous appelez ce script à partir d'un autre script ou de manière automatique, vous pouvez souhaitez désactiver l'invite interactive. La sortie est visible dans le fichier `get_metrics_retention.sh_AAAAMMJJHHMM.log`.

-retention *BEST_PRACTICES|8DAYS|2DAYS|CURRENT*
Appliquez les valeurs de conservation de données recommandées (best practices), 8 jours ou 2 jours à la base de données d'historique. Ce paramètre n'est pas utilisé si vous spécifiez le paramètre **-history**.

-server *nom_hôte_serveur_base_de_données*
Lorsque votre serveur Cloud APM se connecte à un serveur Db2 distant plutôt qu'au serveur Db2 local par défaut, spécifiez l'adresse IP ou le nom d'hôte qualifié complet du serveur Db2.

Référence associée:

«Utilisateurs et mots de passe par défaut», à la page 1075
Des ID utilisateur et mots de passe par défaut sont disponibles pour accéder à certains composants.

Chapitre 2, «Documentation au format PDF», à la page 29
Des documents PDF compilent les rubriques de cette collection IBM Knowledge Center sous la forme de guides d'utilisation. Des références sont également disponibles pour chaque agent.

Seuils d'événement pour la surveillance des transactions

Vous pouvez utiliser des seuils d'événement afin de surveiller immédiatement votre environnement. Vous pouvez également créer des seuils d'événement personnalisés qui testent certaines conditions et déclenchent un événement lorsque des indicateurs clés de performance dépassent le seuil défini.

Evénements de Surveillance des temps de réponse

Des événements de temps de réponse sont créés lorsque des transactions Web dépassent un seuil de **temps de réponse**.

Après avoir cliqué sur  **Configuration système** > **Gestionnaire de seuils**, sélectionnez **Temps de réponse** comme **type de source de données**. Tous les seuils d'événement de l'environnement de Surveillance des temps de réponse sont appliqués à l'ensemble des systèmes gérés de même type.

Les seuils prédéfinis suivants sont disponibles pour l'agent Surveillance des temps de réponse.

Tableau 209. Seuils de Surveillance des temps de réponse

Seuil	Description	Formule
`Response_Time_Availability_Crit`	Un pourcentage élevé de transactions Web a échoué.	Si la transaction WRT Status.Percent_Failed est supérieure à 10 et que la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Availability_Crit est vrai
`Response_Time_Availability_Warn`	Un pourcentage moyen de transactions Web a échoué.	Si la transaction WRT Status.Percent_Failed est supérieure à 0 et que la transaction WRT Status.Percent_Failed est inférieure à 10 et la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Availability_Warn est vrai
`Response_Time_Critical`	Un pourcentage élevé de transactions Web présente un temps de réponse lent.	Si la transaction WRT Status.Percent_Slow est supérieure à 5 et que la transaction WRT Status.Percent_Available est égale à 100 et la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Critical est vrai
`Response_Time_Warning`	Un pourcentage modéré de transactions Web présente un temps de réponse lent.	Si la transaction WRT Status.Percent_Slow est supérieure à 1 et que la transaction WRT Status.Percent_Slow est inférieure à 5, la transaction WRT Status.Percent_Available est égale à 100 et la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Warning est vrai

demandes correctes ont un temps de réponse inférieur à 10 secondes. Les *demandes lentes* ont un temps de réponse supérieur à 10 secondes. La valeur de 10 secondes utilisée pour déterminer si le temps de réponse est correct ou lent n'est pas configurable.

Evénements de Suivi des transactions

Des événements de Suivi des transactions sont créés lorsque des transactions de middleware dépassent un seuil de Suivi des transactions.

Pour afficher les seuils de Suivi des transactions par défaut, cliquez sur  **Configuration système** > **Gestionnaire de seuils** et sélectionnez **Suivi des transactions** comme **type de source de données**.

Conseil : Au besoin, vous pouvez créer vos propres seuils de Suivi des transactions.

Les seuils prédéfinis suivants sont disponibles pour des transactions de middleware.

Tableau 210. Seuils de Suivi des transactions

Seuil	Description	Formule
`Interaction_Avail_Critical`	Un pourcentage élevé d'interactions de middleware a échoué.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 10 alors Interaction_Avail_Critical est vrai
`Interaction_Avail_Warning`	Un pourcentage moyen d'interactions de middleware a échoué.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 0 et que KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est inférieur ou égal à 10 alors `Interaction_Avail_Warning` est vrai
`Interaction_Time_Critical`	Un pourcentage élevé d'interactions de middleware présente un temps total lent.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur ou égal à 5 et que KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Interaction_Time_Critical est vrai
`Interaction_Time_Warning`	Un pourcentage modéré d'interactions de middleware présente un temps total lent.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur à 1 et que KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW est inférieur à 5 et KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Interaction_Time_Warning est vrai
`Transaction_Avail_Critical`	Un pourcentage élevé de transactions de middleware a échoué.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 10 alors Transaction_Avail_Critical est vrai
`Transaction_Avail_Warning`	Un pourcentage moyen de transactions de middleware a échoué.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 0 et que KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est inférieur ou égal à 10 alors `Transaction_Avail_Warning` est vrai
`Transaction_Time_Critical`	Un pourcentage élevé de transactions de middleware présente un temps total lent.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur ou égal à 5 et que KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Transaction_Time_Critical est vrai

Tableau 210. Seuils de Suivi des transactions (suite)

Seuil	Description	Formule
`Transaction_Time_Warning`	Un pourcentage modéré de transactions de middleware présente un temps total lent.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur à 1 et que KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW est inférieur à 5 et KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Transaction_Time_Warning est vrai

demandes correctes ont un temps de réponse inférieur à 10 secondes. Les *demandes lentes* ont un temps de réponse supérieur à 10 secondes. La valeur de 10 secondes utilisée pour déterminer si le temps de réponse est correct ou lent n'est pas configurable.

Création de seuils de génération d'événements pour la surveillance des transactions

Utilisez le gestionnaire de seuils pour créer des seuils pour des transactions. Les seuils sont utilisés pour comparer la valeur d'échantillon d'un attribut avec la valeur définie dans le seuil. Si la valeur d'échantillon répond à la comparaison, un événement de transaction est généré.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des seuils pour déterminer quand les applications signalent des conditions spécifiques. Pour plus d'informations sur les seuils par défaut pour la surveillance des transactions, voir «Seuils d'événement pour la surveillance des transactions», à la page 1045.

Vous pouvez créer des seuils supplémentaires pour surveiller d'autres aspects d'une transaction. Par exemple, vous pouvez créer un seuil afin de surveiller le débit des événements de transaction du middleware. Et, si ce débit passe au-dessous du seuil spécifié, générer un événement.

Procédure

Pour créer un seuil et l'associer à une ou plusieurs transactions, procédez comme suit :

1. Dans la barre de navigation, cliquez sur l'icône **Configuration système** > **Gestionnaire de seuils**. Définissez le **type de source de données** en tant que **suivi des transactions**.
2. Cliquez sur Ajouter pour créer un nouveau seuil.
3. Définissez une gravité pour l'événement qui dépasse ce seuil.
4. Pour associer le seuil à une transaction, définissez les valeurs suivantes :
   - Ensemble de données - `DONNEES AGREGATION TRANSACTION KTE`
   - Elément affiché - `valeur_ressource`
   - Opérateur logique - `And (&)`
5. Alternativement, pour associer le seuil à une interaction, définissez les valeurs suivantes :
   - Ensemble de données - `KTE INTERACTION AGGREGATE DATA`
   - Elément affiché - `Source_Resource_Value`
   - Opérateur logique - `And (&)`
6. Cliquez sur **Ajouter** pour ajouter une condition. Dans la zone **Ajouter une condition**, sélectionnez un attribut et un opérateur, puis entrez une valeur de seuil.

Par exemple, pour ajouter une condition de seuil qui génère un événement de transaction lorsque le nombre de transactions par minute passe au-dessous de 100, définissez les valeurs suivantes, puis cliquez sur **OK**:

- Attribut - `débit_transactions`
- Opérateur - `Inférieur à`
- Valeur - `100`

Au besoin, répétez cette procédure pour ajouter d'autres conditions à votre seuil.

7. Dans la section Affectation de groupes, sélectionnez `Suivi des transactions` pour affecter le seuil à ce groupe de ressources.
8. Cliquez sur **Sauvegarder**.

Résultats

Vous venez de créer un seuil et vous l'avez associé à une transaction ou une interaction. Lorsque les conditions de seuil sont remplies, un événement est généré. Vous pouvez surveiller des événements dans l'onglet Evénements du tableau de bord des performances des applications.

Exemple

Pour créer des seuils pour l'agent Response Time Monitoring en vue de surveiller d'autres aspects d'une transaction Web en plus de ceux surveillés par défaut, procédez comme suit :

1. Dans le gestionnaire de seuils, associez le **type de source de données** à **Temps de réponse**.
2. Lorsque vous ajoutez le seuil, utilisez les paramètres suivants :
   - Ensemble de données - `Statut de transaction WRT`
   - Elément affiché - `Application`
   - Opérateur logique - `And (&)`
   - Affectation de groupes - `Temps de réponse Web`

Gestion des événements d'agent de système d'exploitation

Vous pouvez configurer l'agent de système d'exploitation pour gérer les événements.

Filtrage et récapitulatif des événements

Utilisez les options de filtrage et de récapitulatif des événements définies dans le fichier de configuration (`.conf`) pour contrôler la manière dont les événements en double sont traités par l'agent de système d'exploitation.

Lorsqu'un journal est surveillé, un événement peut rapidement s'afficher plusieurs fois. Cela peut se produire lorsque l'application qui génère le journal détecte une erreur et la consigne en continu jusqu'à ce que le seuil soit atteint. Lorsque ce type de consignation se produit, un nombre d'événements excessif est envoyé à l'infrastructure de Performance Management. Le volume d'événements a un impact négatif sur les performances.

Remarque : Les procédures de détection et de regroupement des événements sont prises en charge uniquement pour les événements envoyés à Performance Management. Vous ne pouvez donc pas exécuter ces procédures avec des événements envoyés à OMNIbus par la fonction EIF.

Détection et filtrage des événements en double

Vous pouvez configurer l'agent de système d'exploitation pour traiter les événements en double.

Pour résoudre le problème d'événements en double, vous devez définir ce que vous considérez comme des doublons dans le fichier `.conf` à l'aide de la balise `DupDetectionKeyAttributes`. Dans une liste séparée par des virgules, vous devez inclure un ou plusieurs attributs Performance Management définis

que vous souhaitez utiliser pour déterminer si un événement est considéré comme un doublon. Dans l'exemple suivant, les événements possédant le même message et le même paramètre `CustomSlot1` sont considérés comme des doublons :

```
DupDetectionKeyAttributes=msg,CustomSlot1
```

Les événements en double sont détectés à partir des attributs Performance Management. Si vous souhaitez que la détection des doublons s'effectue sur des attributs spécifiques définis par vos soins, procédez comme suit :

1. Mappez la valeur d'attribut à un attribut Performance Management.
2. Mappez l'attribut Performance Management à la balise `DupDetectionKeyAttributes` dans le fichier `.conf`.

Dans l'exemple suivant, les attributs importants `eventclass` et `eventid` sont mappés aux paramètres *CustomSlot1* et *CustomSlot2* :

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2}
 [0-9] {4}) [0-9] (\S+) (\S+) \
Microsoft-Windows-Security-Auditing (\S+) ([0-9]+) (.*)
timestamp $1
severity $2
eventclass $3 CustomSlot1
eventkeywords $4
eventid $5 CustomSlot2
msg $6
END
```

Si vous souhaitez définir certains événements comme des doublons, mappez les attributs Performance Management à la balise `DupDetectionKeyAttributes` dans le fichier `.conf`, comme indiqué ci-après :

```
DupDetectionKeyAttributes=CustomSlot1,CustomSlot2
```

Remarque :

1. Les noms d'attribut `CustomSlot` sont sensibles à la casse. Vous devez donc entrer le nom exactement comme décrit dans l'exemple précédent.
2. Si vous n'indiquez pas de liste d'attributs, les valeurs correspondent par défaut à `Class` et `Logname`.

Les événements pour lesquels ces attributs ont une correspondance sont considérés comme des doublons par l'agent.

Etant donné que la détection des doublons est globale, il est recommandé de choisir un ensemble d'attributs personnalisés (CustomSlots) à utiliser en tant que clés et de les utiliser de cette façon dans l'ensemble des instructions de formatage. Par exemple, vous pouvez utiliser les attributs 1 à 3 pour les clés. Si un format a besoin d'une seule clé et de plusieurs attributs, vous pouvez utiliser l'attribut 1 pour contenir la valeur de nom et les attributs 4 à n pour contenir les autres données.

Intervalle de récapitulatif

L'intervalle de récapitulatif désigne la période pendant laquelle s'exécute la procédure de détection de doublons.

Les événements en double sont comptabilisés au cours de cet intervalle à l'issue duquel ils sont réinitialisés. Le compteur recommence le décompte à partir de zéro au début de chaque nouvel intervalle de récapitulatif.

L'agent envoie un événement récapitulatif pour chaque événement défini qu'il surveille au cours de l'intervalle. L'événement récapitulatif contient les valeurs d'attribut du premier événement correspondant. Il contient également le nombre de doublons de cet événement qui se sont produits au cours de l'intervalle de récapitulatif.

L'intervalle de récapitulatif est défini dans le fichier de configuration (`.conf`) comme indiqué dans l'exemple suivant :

```
EventSummaryInterval=300
```

La valeur de l'intervalle de récapitulatif est exprimée en secondes. Dans cet exemple, l'intervalle de récapitulatif est donc de cinq minutes (300 / 60 = 5).

Filtrage des événements

Si le filtrage des événements est en cours d'exécution, le paramètre EventFloodThreshold du fichier (`.conf`) indique à l'agent quand l'événement est envoyé.

Le tableau suivant présente les valeurs EventFloodThreshold.

Tableau 211. Valeurs EventFloodThreshold

Valeurs EventFloodThreshold	Description
send_all	Le paramètre *send_all* est la valeur par défaut. Tous les événements sont envoyés (y compris les doublons).
send_none	Aucun événement n'est envoyé. Seuls les événements récapitulatifs sont envoyés.
send_first	Seul le premier événement rencontré est envoyé. Si des doublons se produisent sur une période spécifique, ils ne sont pas envoyés. Pour plus d'informations, voir «Intervalle de récapitulatif», à la page 1050.
n entier	L'événement est envoyé toutes les *n* occurrences (tous les *5* doublons, par exemple). Pour plus d'informations, voir «Intervalle de récapitulatif», à la page 1050.

Attributs de récapitulation

Les attributs Type d'événement et Nombre d'occurrences sont utilisés pour récapituler les événements.

Les attributs Type d'événement et Nombre d'occurrences prennent tout leur sens dans la récapitulation d'événements. L'attribut Type d'événement indique le type de l'événement (*Evénement* ou *Evénement récapitulatif*). Les événements généraux qui constituent des correspondances un à un d'événements trouvés dans le journal sont de type *Evénement*. Les événements récapitulatifs qui sont envoyés à l'issue de l'intervalle de récapitulatif sont de type *Evénement récapitulatif*.

L'attribut Nombre d'occurrences précise le volume total d'enregistrements en double trouvés dans le journal pour l'événement. Les événements récapitulatifs incluent ce nombre, car il indique le nombre d'événements reçus qui correspondaient à l'événement récapitulatif au cours de l'intervalle de récapitulatif précédent.

Seuils et événements récapitulatifs

Quelle que soit la valeur de filtre (pour les valeurs possibles, voir «Filtrage des événements»), les événements récapitulatifs figurent toujours à la fin de chaque intervalle de récapitulatif, pour tout événement qui s'est produit au moins une fois au cours de cet intervalle. Si vous n'attendez pas d'événements récapitulatif, les seuils peuvent être déclenchés accidentellement. Pour éviter le déclenchement accidentel d'un seuil, incluez une clause dans le seuil pour *`Type d'événement== Evénement`* ou *`Type d'événement!= Evénement récapitulatif`*.

Journal des événements Windows

L'agent de système d'exploitation utilise le fichier .conf pour surveiller les événements consignés dans l'historique des événements Windows.

L'agent de système d'exploitation continue à utiliser l'option WINEVENTLOGS du fichier de configuration (.conf) pour surveiller les événements consignés dans le journal des événements Windows. L'agent surveille une liste de journaux d'événements séparés par des virgules, comme indiqué dans l'exemple suivant :

```
WINEVENTLOGS=System,Security,Application
```

L'agent de système d'exploitation continue également d'utiliser le paramètre WINEVENTLOGS=All. Le paramètre All fait référence aux journaux d'événements standard suivants fournis avec les versions Windows antérieures à 2008 : Sécurité, Application, Système, Active Directory, DNS (Domain Name System) et FRS (File Replication Service). Cependant, tous les journaux des événements système ne sont pas vérifiés.

La balise du fichier de configuration UseNewEventLogAPI permet au journal des événements (journal des événements Windows 2008 ou version ultérieure) d'accéder à tous les nouveaux journaux ajoutés par Microsoft, ainsi qu'à l'ensemble des journaux d'événements Windows créés par d'autres applications ou par l'utilisateur. Les nouveaux journaux sont définis par le mot clé WINEVENTLOGS.

Dans l'exemple suivant, la balise UseNewEventLogAPI a pour valeur y.

```
UseNewEventLogAPI=y
WINEVENTLOGS=Microsoft-Windows-Hyper-V-Worker-Admin
```

Dans cet exemple, le journal Microsoft-Windows-Hyper-V/Admin est surveillé sur un système Windows possédant le rôle Hyper-V.

Dans le journal des événements Windows, chaque événement comporte les zones suivantes dans cet ordre :

- Date au format mois, jour, heure et année
- Catégorie d'événement sous forme d'entier
- Niveau d'événement
- Identificateur de sécurité Windows. Dans l'identificateur de sécurité Windows, tous les espaces sont remplacés par un trait de soulignement si le fichier de configuration (.conf) inclut le paramètre SpaceReplacement=TRUE.

  Remarque : SpaceReplacement=TRUE est la valeur par défaut si vous associez UseNewEventLogAPI à y dans le fichier (.conf) (en indiquant que vous utilisez le journal d'événements).
- Source Windows. Dans le source Windows, tous les espaces sont remplacés par un trait de soulignement si le fichier de configuration (.conf) comporte le paramètre SpaceReplacement=TRUE.
- Mots clés du journal d'événements Windows. Dans les mots clés du journal d'événements Windows, tous les espaces sont remplacés par un trait de soulignement si le fichier de configuration (.conf) inclut le paramètre SpaceReplacement=TRUE.

  Remarque : La zone de mots clés qui est décrite ici est nouvelle dans la version Windows 2008 du journal des événements. Etant donné qu'elle n'existait pas dans les précédentes versions du journal des événements, vous ne pouvez pas réutiliser directement vos anciennes instructions de format du journal des événements. Vous devez d'abord les modifier pour prendre en compte cette nouvelle zone.
- Identificateur d'événement Windows
- Texte du message

Par exemple, lorsqu'un administrateur se connecte à un système Windows 2008, un événement est généré dans le journal de sécurité, indiquant les privilèges associés à la session du nouvel utilisateur :

```
Mar 22 13:58:35 2011 1 Information N/A Microsoft-Windows-
Security-Auditing Audit_Success 4672 Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
```

```
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Pour capturer tous les événements qui ont été créés par la source d'événement `Microsoft-Windows-Security-Auditing`, vous devez écrire une instruction de format comme indiqué ci-dessous :

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2} [0-9]
{4}) [0-9] (\S+) (\S+) Microsoft-Windows-Security-Auditing (\S+)
([0-9]+) (.*)
timestamp $1
severity $2
login $3
eventsource "Microsoft-Windows-Security-Auditing"
eventkeywords $4
eventid $5
msg $6
END
```

L'exemple suivant indique les valeurs qui sont affectées aux attributs pour l'exemple d'événement précédent :

```
timestamp=Mar 22 13:58:35 2011
severity=Information
login=N/A
eventsource=Microsoft-Windows-Security-Auditing
eventid=4672
msg="Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Comme il est difficile d'anticiper l'apparence de ces événements, vous pouvez écrire vos expressions régulières en capturant les événements réels dans un fichier. Il ne vous restera plus ensuite qu'à examiner le fichier, sélectionner les événements devant être capturés par l'agent et écrire les expressions régulières correspondant à ces événements. Pour capturer tous les événements à partir du journal des événements Windows, procédez comme suit :

1. Créez un fichier de format contenant un seul modèle qui ne correspond à rien. Par exemple :

   ```
   REGEX NoMatch
   This doesn't match anything
   END
   ```

2. Dans le fichier de configuration (`.conf`), ajoutez le paramètre :

   ```
   UnmatchLog=C:/temp/evlog.unmatch
   ```

3. Exécutez l'agent et capturez quelques événements échantillonnés.

Mappage d'événements

L'interface Tivoli Event Integration Facility (EIF) permet de réacheminer des événements de situation vers Tivoli Netcool/OMNIbus, Tivoli Enterprise Console ou Operations Analytics - Log Analysis.

Les événements EIF spécifient une classe d'événement et les données d'événement sont spécifiées sous la forme de paires nom/valeur identifiant le nom et la valeur d'un attribut d'événement. Une classe d'événement peut comporter des sous-classes. Performance Management fournit les définitions de classe d'événement de base ainsi qu'un ensemble d'emplacements de base inclus dans tous les événements de surveillance. Les agents étendent les classes d'événement de base afin de définir des sous-classes incluant des attributs spécifiques à l'agent. Pour les événements des fichiers journaux d'agent de système

d'exploitation, les classes d'événement correspondent aux groupes d'attributs d'agent et les attributs d'agent correspondent aux attributs dans le groupe d'attributs.

Pour les événements générés par des seuils dans le groupe d'attributs LFAProfiles, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LFAPROFILES. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- subnode_msn : STRING
- subnode_affinity : STRING
- subnode_type : STRING
- subnode_resource_name : STRING
- subnode_version : STRING
- subnode_config_file : STRING
- subnode_description : STRING
- subnode_description_enum : STRING

Pour les événements générés par des seuils dans le groupe d'attributs Log File RegEx Statistics, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOG_FILE_REGEX_STATISTICS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- table_name : STRING
- attrib_name : STRING
- filter_number : INTEGER
- average_processor_time : REAL
- average_processor_time_enum : STRING
- total_processor_time : REAL
- total_processor_time_enum : STRING
- max_processor_time : REAL
- max_processor_time_enum : STRING
- min_processor_time : REAL
- min_processor_time_enum : STRING
- filter_count : REAL
- filter_count_matched : REAL
- filter_count_unmatched : REAL
- regex_pattern : STRING
- last_matched_time : STRING
- last_matched_time_enum : STRING
- last_unmatched_time : STRING
- last_unmatched_time_enum : STRING
- result_type : INTEGER
- result_type_enum : STRING

Pour les événements générés par des seuils dans le groupe d'attributs Log File Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOG_FILE_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- table_name : STRING
- file_name : STRING
- regex_pattern : STRING
- file_type : INTEGER
- file_type_enum : STRING
- file_status : INTEGER
- file_status_enum : STRING
- num_records_matched : INTEGER
- num_records_not_matched : INTEGER
- num_records_not_matched_enum : STRING
- num_records_processed : INTEGER
- current_file_position : REAL
- current_file_position_enum : STRING
- current_file_size : REAL
- current_file_size_enum : STRING
- last_modification_time : STRING
- last_modification_time_enum : STRING
- codepage : STRING

Pour les événements générés par des seuils dans le groupe d'attributs LogfileEvents, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOGFILEEVENTS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- klo_class : STRING
- logname : STRING
- eifevent : STRING
- klo_msg : STRING
- customslot1 : STRING
- customslot2 : STRING
- customslot3 : STRING
- customslot4 : STRING
- customslot5 : STRING
- customslot6 : STRING
- customslot7 : STRING
- customslot8 : STRING
- customslot9 : STRING
- customslot10 : STRING
- occurrence_count : INTEGER
- occurrence_count_enum : STRING
- event_type : INTEGER
- event_type_enum : STRING
- custominteger1 : REAL
- custominteger1_enum : STRING

- custominteger2 : REAL
- custominteger2_enum : STRING
- custominteger3 : REAL
- custominteger3_enum : STRING
- remotehost : STRING

Pour les événements générés par des seuils dans le groupe d'attributs LogfileProfileEvents, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOGFILEPROFILEEVENTS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- klo_class : STRING
- logname : STRING
- eifevent : STRING
- klo_msg : STRING
- customslot1 : STRING
- customslot2 : STRING
- customslot3 : STRING
- customslot4 : STRING
- customslot5 : STRING
- customslot6 : STRING
- customslot7 : STRING
- customslot8 : STRING
- customslot9 : STRING
- customslot10 : STRING
- occurrence_count : INTEGER
- occurrence_count_enum : STRING
- event_type : INTEGER
- event_type_enum : STRING
- custominteger1 : REAL
- custominteger1_enum : STRING
- custominteger2 : REAL
- custominteger2_enum : STRING
- custominteger3 : REAL
- custominteger3_enum : STRING
- remotehost : STRING

Pour les événements générés par des seuils dans le groupe d'attributs Performance Object Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_PERFORMANCE_OBJECT_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- query_name : STRING
- object_name : STRING
- object_type : INTEGER
- object_type_enum : STRING

- object_status : INTEGER
- object_status_enum : STRING
- error_code : INTEGER
- error_code_enum : STRING
- last_collection_start : STRING
- last_collection_start_enum : STRING
- last_collection_finished : STRING
- last_collection_finished_enum : STRING
- last_collection_duration : REAL
- average_collection_duration : REAL
- average_collection_duration_enum : STRING
- refresh_interval : INTEGER
- number_of_collections : INTEGER
- cache_hits : INTEGER
- cache_misses : INTEGER
- cache_hit_percent : REAL
- intervals_skipped : INTEGER

Pour les événements générés par des seuils dans le groupe d'attributs pro Performance Object Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_PRO_PERFORMANCE_OBJECT_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- query_name : STRING
- object_name : STRING
- object_type : INTEGER
- object_type_enum : STRING
- object_status : INTEGER
- object_status_enum : STRING
- error_code : INTEGER
- error_code_enum : STRING
- last_collection_start : STRING
- last_collection_start_enum : STRING
- last_collection_finished : STRING
- last_collection_finished_enum : STRING
- last_collection_duration : REAL
- average_collection_duration : REAL
- average_collection_duration_enum : STRING
- refresh_interval : INTEGER
- number_of_collections : INTEGER
- cache_hits : INTEGER
- cache_misses : INTEGER
- cache_hit_percent : REAL
- intervals_skipped : INTEGER

Pour les événements générés par des seuils dans le groupe d'attributs Thread Pool Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_THREAD_POOL_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- thread_pool_size : INTEGER
- thread_pool_size_enum : STRING
- thread_pool_max_size : INTEGER
- thread_pool_max_size_enum : STRING
- thread_pool_active_threads : INTEGER
- thread_pool_active_threads_enum : STRING
- thread_pool_avg_active_threads : REAL
- thread_pool_avg_active_threads_enum : STRING
- thread_pool_min_active_threads : INTEGER
- thread_pool_min_active_threads_enum : STRING
- thread_pool_max_active_threads : INTEGER
- thread_pool_max_active_threads_enum : STRING
- thread_pool_queue_length : INTEGER
- thread_pool_queue_length_enum : STRING
- thread_pool_avg_queue_length : REAL
- thread_pool_avg_queue_length_enum : STRING
- thread_pool_min_queue_length : INTEGER
- thread_pool_min_queue_length_enum : STRING
- thread_pool_max_queue_length : INTEGER
- thread_pool_max_queue_length_enum : STRING
- thread_pool_avg_job_wait : REAL
- thread_pool_avg_job_wait_enum : STRING
- thread_pool_total_jobs : INTEGER
- thread_pool_total_jobs_enum : STRING

Gestion des transactions et des événements synthétiques

Créez des transactions synthétiques qui surveillent les performances et la disponibilité des applications internes et des applications externes.

Créez une *transaction synthétique* dans Synthetic Script Manager. Générez des scripts simples dans Synthetic Script Manager pour tester la disponibilité d'une application, ou utilisez Selenium IDE pour enregistrer des scripts synthétiques répliquant différentes actions utilisateur effectuées sur une application. Configurez ensuite une transaction synthétique pour exécuter votre script à des intervalles et des emplacements d'exécution spécifiques.

Vos emplacements d'exécution disponibles sont les emplacements où vous avez installé l'Monitoring Agent for Synthetic Playback.

Créez des seuils et des groupes de ressources pour déclencher des événements et notifier les parties prenantes lorsque vos applications sont lentes ou indisponibles. Visualisez les données de performance et générez des rapports d'historique dans le Tableau de bord d'Application Performance.

Si vous surveillez le temps de réponse utilisateur final d'une application à l'aide de l'agent Temps de réponse, vous pouvez afficher les indicateurs clés de performance des transactions utilisateur final et

synthétiques dans le Tableau de bord d'Application Performance. Ajoutez les transactions synthétiques en tant que composants à l'application que vous surveillez avec l'agent Temps de réponse.

Remarque : Pour travailler dans Synthetics Script Manager, vous devez être membre d'un rôle qui dispose du droit d'affichage pour Synthetic Script Manager et Configuration d'agent. Pour plus d'informations, voir «Rôles et droits», à la page 1021.

Enregistrement de scripts synthétiques

Enregistrez un script synthétique à l'aide du navigateur Web Firefox et du module complémentaire Selenium IDE.

Avec Selenium IDE, vous pouvez enregistrer des actions utilisateur sur une page Web, telles que le chargement d'une page, l'activation d'un lien ou la sélection d'un objet. Lorsque Selenium IDE procède à l'enregistrement, il génère une commande pour chaque action utilisateur dans un script. Ensuite, à l'aide de Synthetic Script Manager, vous pouvez configurer les scripts de sorte à simuler un comportement utilisateur sur votre site Web, à des intervalles définis et à des emplacements différents.

Important : Vous devez utiliser le navigateur Web Firefox lors de l'enregistrement de scripts. Selenium IDE est uniquement disponible en tant que module complémentaire Firefox.

Avant de commencer

Si Selenium IDE n'est pas installé ou en cours d'exécution, procédez comme suit :

1. Vérifiez que vous exécutez une version de Firefox prenant en charge Selenium IDE.

   Remarque : Selenium IDE ne fonctionne pas sous Firefox v55 et versions ultérieures. Pour plus d'informations, voir https://addons.mozilla.org/en-US/firefox/addon/selenium-ide/.
2. Téléchargez et installez Selenium IDE depuis la page d'accueil de Selenium. Autorisez Selenium IDE à installer tous les plug-in. Lorsque Selenium IDE est installé, redémarrez Firefox.
3. Démarrez le navigateur Web Firefox. Accédez à la page Web que vous souhaitez tester, puis fermez tous les autres onglets. Pour ouvrir Selenium IDE, cliquez sur **Outils** > **Selenium IDE**. Dans la fenêtre Selenium IDE, vérifiez que la zone **Base URL** contient l'adresse URL de la page Web affichée. Selenium IDE commence à enregistrer toutes les actions utilisateur sur la page Web affichée.

Pourquoi et quand exécuter cette tâche

Dans cette tâche, vous effectuez des actions utilisateur sur une page Web et utilisez Selenium IDE pour enregistrer ces actions sous la forme de commandes dans un script simple. Vous pouvez utiliser des scripts pour surveiller les performances et la disponibilité de votre application Web dans le Tableau de bord d'Application Performance.

Procédure

Pour enregistrer un script d'actions utilisateur sur une page Web, procédez comme suit :

1. Cliquez sur **Record** pour démarrer l'enregistrement d'un script. Effectuez des actions utilisateur sur votre page Web, par exemple, cliquer sur un lien. Pour chaque action utilisateur sur une page Web, Selenium IDE enregistre une commande et l'ajoute à un script.

   Ainsi, pour enregistrer dans un script le chargement par un utilisateur de la page Web IBM Marketplace et avoir accès à un essai gratuit de Cloud APM, procédez comme suit :

Tableau 212. Actions utilisateur enregistrées et commandes Selenium IDE

Action utilisateur	Commandes ajoutées au script
Pour enregistrer à quel moment la page Web Cloud APM sur le site Web IBM Marketplace s'ouvre, ouvrez la page Web IBM Marketplace. Cliquez avec le bouton droit de la souris sur un point quelconque de la page Web affichée, puis sélectionnez **open**.	`open`
Pour vérifier que le script contrôle le chargement de la page Web, cliquez avec le bouton droit de la souris sur le titre de la page Web (IBM Cloud Application Performance Management), puis cliquez sur **Afficher toutes les commandes disponibles** > **verifyTitle IBM Cloud Application Performance Management**.	`verifyTitle`
Pour enregistrer à quel moment l'utilisateur clique sur un lien pour afficher des détails sur Cloud APM, cliquez sur le lien **Détails**. La page Détails se charge.	`clickAndWait`
Pour vérifier que le script contrôle le chargement de la page Web Détails, cliquez avec le bouton droit de la souris sur l'en-tête «Feature spotlights» et sélectionnez **Afficher toutes les commandes disponibles** > **verifyText css=h2.heading--TERTIARY**.	`verifyText`
Pour enregistrer à quel moment l'utilisateur clique sur un lien pour afficher des détails relatifs à l'achat de Cloud APM, cliquez sur le lien **Acheter**. La page Acheter se charge.	`clickandWait`
Pour enregistrer les clics de l'utilisateur sur le bouton permettant de s'inscrire pour un essai gratuit de Cloud APM, cliquez sur le bouton **Essai gratuit**.	`click`

2. Dans la fenêtre Selenium IDE, cliquez sur **Record** pour arrêter l'enregistrement. Cliquez sur **Fichier** > **Sauvegarder le scénario de test en tant que**. Attribuez un nom significatif à votre script et sauvegardez le script en tant que fichier `.html` ; par exemple `open_webpage.html`.
3. Dans la fenêtre Selenium IDE, passez en revue le script enregistré. Cliquez sur l'onglet **Table** pour afficher le script dans un tableau. Dans la fenêtre Selenium IDE, cliquez sur **Play Current Test Case** pour tester la diffusion du script que vous avez enregistré.

   Dans cet exemple, Selenium IDE affiche le script des actions utilisateur sur le site Web IBM Marketplace, comme indiqué à l'étape 1.

Tableau 213. Exemple d'enregistrement de script Selenium IDE consignant les actions utilisateur sur le site Web IBM Marketplace

Commande	Cible	Valeur
`open`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	
`clickAndWait`	`css=ul > #details > a`	
`verifyText`	`css=h2.heading--TERTIARY`	Feature spotlights
`clickAndWait`	`css=ul > #purchase > a`	
`click`	`link=Essai gratuit`	

Résultats

Vous venez d'enregistrer un script que vous pouvez utiliser pour surveiller les performances et la disponibilité d'une application Web.

Que faire ensuite

Si vous avez enregistré un script complexe, vous pouvez organiser votre script en scripts plus simples. Chaque script représentera un processus métier ou une action utilisateur spécifique sur votre application Web.

Utilisez Synthetic Script Manager pour transférer votre fichier script vers une transaction synthétique nouvelle ou existante.

Structuration des scripts complexes

Organisez un script complexe en plusieurs scripts, puis sauvegardez les scripts ensemble dans une collection de scripts.

Pourquoi et quand exécuter cette tâche

Si vous créez un script complexe, vous pouvez l'organiser en plusieurs scripts simples qui représentent différents processus métier ou utilisateur dans votre application Web. Sauvegardez les scripts ensemble en tant que suite de tests. Vous pouvez alors utiliser ces scripts pour surveiller les performances et la disponibilité de votre application Web en réponse à des actions utilisateur spécifiques dans le Tableau de bord d'Application Performance.

Important : Il est recommandé d'organiser les scripts complexes en scripts distincts, chaque script représentant un processus utilisateur ou métier spécifique à surveiller. Par exemple, créez des scripts distincts qui enregistrent la recherche d'un élément ou la connexion, par un utilisateur, à un site Web. Si vous organisez vos scripts par processus utilisateur ou métier, vous pouvez alors surveiller la réponse de votre application Web à ces processus spécifiques dans le Tableau de bord d'Application Performance.

Procédure

Pour organiser un script complexe en scripts distincts et sauvegarder vos scripts en tant que suite de tests, procédez comme suit :

1. Pour créer un script distinct pour chaque processus utilisateur enregistré dans votre script, cliquez sur **Fichier** > **Nouveau scénario de test** dans Selenium IDE. Attribuez à chaque script un nom significatif décrivant le processus utilisateur et sauvegardez chaque script en tant que fichier `.html` ; par exemple `load_homepage.html`. Pour plus d'informations, voir «Enregistrement de scripts synthétiques», à la page 1059.

   Important : Le nom attribué à votre script dans Selenium IDE est le nom qui identifie le processus métier ou utilisateur enregistré que vous surveillez dans le Tableau de bord d'Application Performance.
2. Dans Selenium IDE, ouvrez un script complexe déjà enregistré. Organisez vos commandes de script dans des scripts distincts, en fonction des différentes actions utilisateur. **Coupez** les commandes dans le script complexe initial dans la fenêtre Scénario de test, et **collez**-les dans les différents scripts. Sauvegardez à nouveau chacun des scripts.

   Par exemple, l'exemple de script complexe de la rubrique Enregistrement de scripts synthétiques contient les commandes Selenium IDE associées aux trois processus utilisateur possibles.
   - Ouvrez la page d'accueil Cloud APM sur le site Web IBM Marketplace.
   - Ouvrez la page Details sur IBM Marketplace.
   - Ouvrez la page Tarification et enregistrez l'ouverture par l'utilisateur de la page d'inscription à un essai gratuit.

Les actions utilisateur sont alors organisées selon trois scripts distincts.

Tableau 214. Exemple de script correspondant à l'ouverture de la page IBM Marketplace (load_homepage.html)

Commande	Cible	Valeur
open	/	
verifyTitle	IBM Cloud Application Performance Management	

Tableau 215. Exemple de script correspondant à l'ouverture de la page Details sur IBM Marketplace (load_products.html)

Commande	Cible	Valeur
clickAndWait	css=ul > #details > a	
verifyText	css=h2.heading--TERTIARY	Feature spotlights

Tableau 216. Exemple de script correspondant à l'ouverture de la page Acheter et de la page d'inscription à l'essai dans IBM Marketplace (load_APM.html)

Commande	Cible	Valeur
clickAndWait	css=ul > #purchase > a	
click	link=Essai gratuit	

3. Pour sauvegarder vos fichiers script individuels ensemble dans une suite de tests, cliquez sur **Fichier** > **Sauvegarder la suite de tests en tant que**. Sauvegardez la suite de tests en tant que fichier `.testsuite`. Enfin, compressez la suite de tests et les fichiers script individuels ensemble dans un fichier `.zip`. Le fichier `.zip` doit contenir la suite de tests ainsi que tous les fichiers script inclus dans la suite de tests.

Résultats

Vous venez d'enregistrer un ensemble de scripts que vous pouvez utiliser pour surveiller les performances et la disponibilité de vos applications Web. Utilisez Synthetic Script Manager pour télécharger le fichier `.zip` contenant vos scripts vers une transaction synthétique nouvelle ou existante.

Gestion des transactions synthétiques

Utilisez Synthetic Script Manager pour créer, configurer et supprimer des transactions synthétiques.

Pour afficher Synthetic Script Manager, cliquez sur l'icône **Configuration système** et sélectionnez **Synthetic Script Manager**. Pour travailler dans Synthetics Script Manager, vous devez être membre d'un rôle qui dispose du droit d'affichage pour **Synthetic Script Manager** et **Configuration d'agent**. Pour plus d'informations, voir «Rôles et droits», à la page 1021.

Vous pouvez effectuer les tâches suivantes à l'aide de Synthetic Script Manager :

- Créer et éditer une transaction synthétique.
- Configurer des variables de transaction synthétique.
- Supprimer une transaction synthétique.

Création et édition d'une transaction synthétique :

Pour visualiser les données relatives aux performances et à la disponibilité d'une application Web, vous devez commencer par créer une transaction synthétique dans Synthetic Script Manager.

Pourquoi et quand exécuter cette tâche

Utilisez Synthetic Script Manager pour créer, éditer et configurer une transaction synthétique. Entrez l'adresse URL d'une application Web dans Synthetic Script Editor pour générer un script simple pour votre transaction synthétique. Pour simuler des processus utilisateur complexes, transférez un script synthétique vers une transaction synthétique dans Synthetic Script Editor. Configurez ensuite votre transaction synthétique pour l'exécuter à intervalles réguliers et à différents emplacements.

Procédure

Pour créer une transaction ou éditer une transaction existante, procédez comme suit :

1. Facultatif : Si Synthetic Script Manager n'est pas affiché, cliquez sur l'icône **Configuration système** et sélectionnez **Synthetic Script Manager**.
2. Pour créer une transaction, cliquez sur l'icône **Nouveau** . Pour éditer une transaction existante, cliquez sur l'icône **Editer** .
3. Dans Synthetic Script Editor, cliquez sur l'onglet **Upload a Script** et entrez un nom de transaction dans la zone de texte **Nom de transaction**. Entrez une description de votre transaction dans la zone de texte **Description**.

   Important : N'attribuez pas à votre transaction le même nom que celui d'une transaction que vous avez supprimée ces dernières 24 heures. Sinon, les données issues des deux transactions ne seront pas correctement attribuées à ce nom de transaction dans le Tableau de bord d'Application Performance.
4. Pour générer un script simple afin de tester une application Web, sélectionnez **Enter the URL of web page to test** et entrez une URL. Synthetic Script Manager génère un script synthétique simple en se basant sur cette URL.
5. Pour affecter un fichier script créé précédemment à votre transaction, sélectionnez **Upload script file**. Cliquez sur **Télécharger un script** pour parcourir les scripts sur votre système. Choisissez un script et cliquez sur **Ouvrir**.

   Important : Le fichier script synthétique doit être de l'un des types de fichier suivants :
   - `.html`
   - `.zip`

   Sauvegardez des scripts individuels simples (scénarios de test) sous la forme de fichiers `.html`. Compressez les scénarios de test et les suites de tests ensemble dans un fichier `.zip`.
6. Pour configurer une simulation simultanée ou échelonnée d'une transaction synthétique, cliquez sur l'onglet **Planifier un script**. Sélectionnez **Simultaneous** pour exécuter la transaction à partir de tous les emplacements simultanément, ou **Staggered** pour exécuter la transaction à partir d'un autre emplacement à chaque intervalle.
7. Pour choisir la fréquence d'exécution d'un script, cliquez sur l'onglet **Planifier un script**. Cliquez sur la zone de texte **Intervalle** et saisissez un nombre, en fonction de la fréquence de surveillance souhaitée de votre application Web. Choisissez une durée d'intervalle comprise entre `1` et `60` minutes.

   Remarque : Les scripts volumineux ou complexes peuvent prendre plus de temps à s'exécuter. Choisissez une durée d'intervalle plus longue pour les scripts volumineux ou complexes.
8. Pour choisir les emplacements d'exécution de votre script, cliquez sur l'onglet **Planifier un script**, puis sélectionnez les emplacements d'installation de l'agent où vous voulez exécuter votre script.
9. Pour définir des seuils de temps de réponse pour les transactions et sous-transactions synthétiques, cliquez sur l'onglet **Paramètres avancés** ; cliquez ensuite sur une transaction synthétique et développez-la pour révéler toutes les sous-transactions. Cliquez deux fois sur la valeur du seuil de temps de réponse et entrez une valeur. Choisissez une valeur comprise entre `0` et `3600` secondes. Si vous ne souhaitez pas définir de seuil, entrez `0`. La valeur du seuil de temps de réponse par défaut est 10 secondes.

Remarque : Certaines commandes peuvent prendre plus de temps que d'autres. Choisissez un seuil de temps de réponse qui convient à la commande que vous souhaitez tester. Si votre transaction teste le délai d'ouverture d'une page Web, choisissez un temps de réponse plus long.

10. Pour terminer la création ou l'édition de votre transaction, cliquez sur **Sauvegarder**.

Résultats

Vous venez de configurer une transaction synthétique. La transaction synthétique est à présent répertoriée dans Synthetic Script Manager.

Que faire ensuite

Vous pouvez visualiser les mesures et les indicateurs clés de performance enregistrés par une transaction synthétique dans le Tableau de bord d'Application Performance. Vous pouvez également ajouter des transactions sous la forme de composants à une application et visualiser toutes les transactions synthétiques associées à cette application.

Important : Lorsque vous ajoutez une transaction synthétique pour la première fois, un espace vide peut apparaître dans le widget de groupe Disponibilité dans le temps du Tableau de bord d'Application Performance. L'espace vide disparaît rapidement lorsque le serveur reçoit les premiers résultats de simulation de la transaction.

Configuration des variables de transaction synthétique :

Utilisez Synthetic Script Manager pour mettre à jour des valeurs de variable, telles que des noms et des mots de passe d'utilisateur stockés dans des scripts synthétiques, sans avoir à éditer les fichiers script. Les valeurs des variables doivent être uniques pour chaque site d'exécution.

Configurez des variables pour vos scripts synthétiques lorsque vos applications Web requièrent différentes valeurs de variables sur différents sites. Par exemple, si votre application Web ne permet pas d'avoir les mêmes détails de connexion sur différents sites, utilisez Synthetic Script Manager pour fournir des détails de connexion différents sur chaque site. Vous pouvez créer des variables dans des scripts synthétiques à l'aide de la commande `store` dans le plug-in Selenium-IDE.

Pourquoi et quand exécuter cette tâche

Dans cette tâche, utilisez Synthetic Script Manager pour configurer des variables stockées dans votre script synthétique.

Procédure

Pour configurer les variables d'une transaction synthétique, procédez comme suit :

1. Si Synthetic Script Manager n'est pas affiché, cliquez sur l'icône **Configuration système** et sélectionnez **Synthetic Script Manager**. Sélectionnez une transaction synthétique dans la liste et cliquez sur l'icône **Editer** .
2. Sélectionnez les sites d'exécution de votre transaction synthétique.
3. Cliquez sur l'onglet **Paramètres avancés**. Si le script synthétique contient des variables, vous pouvez éditer ces variables dans la fenêtre Configurer les substitutions de variable pour les différents sites. Pour éditer une variable, cliquez deux fois sur la valeur. Pour terminer, cliquez sur **Sauvegarder**.

   Par exemple, le script suivant contient les variables *nom_d'utilisateur* et *mot_de_passe*. Les valeurs de ces variables, `user1` et `pass`, sont sauvegardées à l'aide de la commande `store` dans Selenium-IDE. Les variables ont la même valeur sur deux sites, Dallas et San Jose.

Tableau 217. Exemple de script contenant des variables

Commande	Cible	Valeur
`store`	`user1`	*nom_d'utilisateur*
`store`	`pass`	*mot_de_passe*
`type`	`id=j_username`	*${nom_d'utilisateur}*
`type`	`id=j_password`	*${mot_de_passe}*

Les valeurs des variables de script sont affichées dans la fenêtre Configurer les substitutions de variable pour les différents emplacements. Remplacez la valeur `user1` de *nom_utilisateur* utilisée sur le site `Dallas` par la valeur `admin1` de sorte que la transaction synthétique utilise des détails de connexion différents sur chaque site.

Tableau 218. Valeurs de variables de script à différents emplacements

Emplacement	nom_d'utilisateur	mot_de_passe
San Jose	user1	pass
Dallas	admin1	pass

Résultats

Vous venez de configurer les variables d'une transaction synthétique. Vous pouvez désormais utiliser cette transaction synthétique pour tester les performances et la disponibilité d'une application Web sur différents sites.

Que faire ensuite

Vous pouvez visualiser les mesures et les indicateurs clés de performance enregistrés par une transaction synthétique dans le Tableau de bord d'Application Performance. Vous pouvez également ajouter des transactions sous la forme de composants à une application et visualiser toutes les transactions synthétiques associées à cette application.

Instructions pour masquer les mots de passe dans Synthetic Script Manager :

Stockez les mots de passe sous forme de variables dans vos scripts synthétiques pour masquer leurs valeurs dans Synthetic Script Manager.

Avant de commencer

Cette procédure requiert la modification d'un script synthétique. Enregistrez un script synthétique à l'aide de Selenium IDE. Pour plus d'informations, voir «Enregistrement de scripts synthétiques», à la page 1059.

Pourquoi et quand exécuter cette tâche

Modifiez manuellement vos scripts synthétiques dans Selenium IDE pour stocker votre mot de passe sous forme de variable. Vous pourrez ensuite créer des transactions synthétiques avec des mots de passe masqués dans Synthetic Script Manager. Les mots de passe masqués s'affichent sous forme d'astérisques dans Synthetic Script Manager.

Important : Il est recommandé de stocker vos mots de passe dans des scripts synthétiques de sorte que leurs valeurs n'apparaissent pas dans Synthetic Script Manager. Les autres utilisateurs ne pouvant pas les voir, les mots de passe masqués offrent une sécurité supplémentaire pour vos applications Web.

Procédure

1. Ouvrez le script que vous voulez modifier dans Selenium-IDE. Utilisez la commande `store` pour affecter un mot de passe à la variable *password*, selon l'exemple décrit dans cette étape. Ensuite, enregistrez le script.

   Important : Vous devez stocker le mot de passe sous le nom de variable *password* afin qu'il ne s'affiche pas dans Synthetic Script Manager.

   Par exemple, le script synthétique ci-dessous contient un nom d'utilisateur *test@example.com* et une valeur de mot de passe *ibm4value*.

   ```
   <tr>
      <td>type</td>
      <td>id=username</td>
      <td>test@example.com</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=password</td>
      <td>ibm4value</td>
   </tr>
   ```

   Le script ci-dessous indique comment affecter la valeur de mot de passe *ibm4value* à la variable *password* à l'aide de la commande `store`.

   ```
   <tr>
      <td>store</td>
      <td>ibm4value</td>
      <td>password</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=username</td>
      <td>test@example.com</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=password</td>
      <td>$(password)</td>
   </tr>
   ```

2. Facultatif : Pour masquer le mot de passe au niveau du script, affectez une valeur vide à la variable *password* à l'aide de la commande `store`, puis enregistrez le script. Vous pouvez définir le mot de passe ultérieurement dans Synthetic Script Manager.

   Par exemple, le script ci-dessous indique comment affecter une valeur vide à la variable *password* à l'aide de la commande `store`.

   ```
   <tr>
      <td>store</td>
      <td></td>
      <td>password</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=username</td>
      <td>test@example.com</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=password</td>
      <td>$(password)</td>
   </tr>
   ```

3. Connectez-vous à la console Cloud APM et ouvrez Synthetic Script Manager. Créez une transaction et téléchargez votre script dans cette transaction. Cliquez sur l'onglet **Paramètres avancés**. Le mot de passe est masqué pour chaque localisation. Vous pouvez modifier le mot de passe pour chaque localisation. Pour plus d'informations, voir «Gestion des transactions synthétiques», à la page 1062.

Suppression d'une transaction synthétique :

Utilisez Synthetic Script Manager pour supprimer des transactions synthétiques.

Procédure

Pour supprimer une transaction synthétique, procédez comme suit :

1. Si une transaction synthétique est affectée à une application, vous devez commencer par supprimer la transaction de cette application. Sur le Tableau de bord d'Application Performance, cliquez sur **Toutes mes applications** et développez, puis cliquez sur l'application qui est associée à la transaction synthétique que vous voulez supprimer. Cliquez sur l'icône **Editer** . Dans la fenêtre Modification d'application, supprimez le composant de transaction synthétique de l'application. Pour plus d'informations, voir Gestion des applications. La transaction synthétique peut désormais être supprimée.
2. Dans la barre de navigation, cliquez sur l'icône **Configuration système** et sélectionnez **Synthetic Script Manager**. Sélectionnez une transaction synthétique, puis cliquez sur l'icône **Supprimer** . Pour confirmer que vous souhaitez supprimer cette transaction synthétique, cliquez sur **OK**.

Résultats

La transaction synthétique est supprimée.

Affichage des données d'une transaction synthétique dans le Tableau de bord d'Application Performance

Affichez les données de transaction synthétique dans le Tableau de bord d'Application Performance. Associez les transactions synthétiques à une application nouvelle ou existante et affichez toutes les transactions synthétiques associées dans le Tableau de bord d'Application Performance.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher les données de transaction synthétique dans la fenêtre My Transactions du Tableau de bord d'Application Performance.

Vous pouvez également créer des groupes de transactions synthétiques en associant vos transactions à une application. Utilisez l'outil Ajouter une application ou Modifier une application du Tableau de bord d'Application Performance pour ajouter des transactions synthétiques sous la forme de composants à une application Web nouvelle ou existante. Vous pouvez ensuite afficher les données de toutes les transactions synthétiques qui sont associées à cette application dans le Tableau de bord d'Application Performance.

Si vous utilisez déjà l'agent Temps de réponse pour surveiller le temps de réponse utilisateur pour une application, vous pouvez ajouter une transaction synthétique à cette application. Vous pouvez alors visualiser des mesures et des indicateurs clés de performance supplémentaires pour cette application dans le Tableau de bord d'Application Performance.

Procédure

- Pour afficher les transactions synthétiques, procédez comme suit :
  1. Cliquez sur l'icône **Performance** et sélectionnez **Tableau de bord d'Application Performance**. Dans la fenêtre Applications, développez **Toutes mes applications** et sélectionnez **My Transactions**. Dans la fenêtre Groupes, développez **Transactions** et sélectionnez **Transactions synthétiques**.
  2. Cliquez sur une transaction synthétique pour afficher les données de disponibilité et de performance de cette transaction, avec un graphique des temps de réponse pour les instances de transaction sur une période définie.
- Pour associer des transactions synthétiques à une application, procédez comme suit :

1. Cliquez sur l'icône **Performance** et sélectionnez **Tableau de bord d'Application Performance**. Sélectionnez et éditez une application existante ou créez une application. Pour plus d'informations, voir Gestion des applications.
2. Dans la fenêtre Ajouter une application, cliquez sur l'icône **Ajouter des composants** et sélectionnez **Transactions synthétiques** dans la liste des composants. Dans la fenêtre Editeur de composants, sélectionnez une transaction synthétique et cliquez sur **Ajouter** pour associer la transaction synthétique à l'application.
3. Cliquez sur **Précédent**. Cliquez sur **Fermer** pour fermer la fenêtre Editeur de composants. Cliquez sur **Sauvegarder**. Pour ajouter une autre transaction synthétique sous la forme d'un composant, répétez les étapes 1 à 3.

Résultats

Vous venez d'associer une transaction synthétique à une application. Vous pouvez désormais afficher l'application et ses transactions synthétiques associées dans le Tableau de bord d'Application Performance. Pour plus d'informations, voir Gestion des applications.

Remarque : Lorsque vous associez une transaction synthétique à une application, la disponibilité initiale de cette application est inconnue. La mise à jour du statut peut prendre plusieurs minutes.

Gestion des événements synthétiques

Utilisez le gestionnaire de seuils et le gestionnaire de groupes de ressources pour configurer les seuils et les affecter à des transactions synthétiques. Les événements synthétiques sont générés lorsque la valeur d'un attribut de transaction correspond à la condition définie dans le seuil. Vous pouvez surveiller les événements synthétiques dans le Tableau de bord d'Application Performance.

Création d'un seuil pour les transactions synthétiques :

Utilisez le gestionnaire de seuils pour créer des seuils destinés aux transactions synthétiques. Les seuils sont utilisés pour comparer les valeurs d'attribut aux valeurs définies dans le seuil. Si la valeur d'échantillon répond à la comparaison, un événement est généré.

Pourquoi et quand exécuter cette tâche

Les seuils permettent aux utilisateurs de surveiller la signalisation de conditions spécifiques par les applications. Par exemple, vous pouvez créer un seuil pour surveiller le délai utilisé par un site Web pour répondre à une commande utilisateur spécifique. Si le site Web met plus de temps que le délai spécifié par votre seuil, un événement synthétique est généré.

Procédure

Pour créer un seuil et l'associer à une ou plusieurs transactions synthétiques, procédez comme suit :

1. Dans la barre de navigation, cliquez sur l'icône **Configuration système** et sélectionnez **Gestionnaire de seuils**. Définissez le type de **source de données** sur **Synthetic Transaction** (Transaction synthétique).
2. Créez un seuil. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1002.
3. Pour associer le seuil à une transaction, sélectionnez **KSO TRANSACTION** comme **Ensemble de données**, puis sélectionnez **TRANSNAME** comme **Elément affiché**. Pour l'**Opérateur logique**, sélectionnez **And (&)**.

   Remarque : Vous devez sélectionner **TRANSNAME** comme **Elément affiché**. Si vous ne sélectionnez pas **TRANSNAME**, vous ne pouvez pas visualiser les événements synthétiques dans le tableau de bord d'Application Performance.

4. Pour ajouter une condition, cliquez sur l'icône **New Condition** . Dans la zone New Condition, sélectionnez un **attribut** et un **opérateur**. Saisissez ensuite une valeur de seuil dans la zone **Valeur**. Pour ajouter cette condition au seuil, cliquez sur **OK**.

   Par exemple, pour ajouter une condition de seuil qui génère un événement synthétique lorsque plus de 50 % des transactions sont lentes, sélectionnez **PSLOW** comme **Attribut** et **Supérieur à** comme **Opérateur**. Pour définir le pourcentage de transactions lentes pour générer un événement, entrez `50` comme **Valeur**.
5. Pour définir plus d'attributs de seuil, ajoutez plus de conditions à votre seuil.
6. Une fois que vous avez terminé, cliquez sur **Sauvegarder**. Si vous ne souhaitez pas affecter le seuil à un groupe de ressources, cliquez sur **OK**.

Résultats

Vous venez de créer un seuil et l'avez associé à une transaction synthétique. Lorsque les conditions de seuil sont remplies, un événement est généré. Vous pouvez surveiller les événements dans l'onglet Evénements du Tableau de bord d'Application Performance.

Que faire ensuite

Vous pouvez regrouper vos transactions synthétiques en groupes de ressources.

Création d'un groupe de ressources pour les transactions synthétiques :

Organisez vos transactions synthétiques dans un groupe de ressources et appliquez des seuils à toutes les transactions de ce groupe de ressources.

Avant de commencer

Créez un seuil à appliquer à toutes les transactions synthétiques de votre groupe de ressources.

Pourquoi et quand exécuter cette tâche

Vous pouvez organiser vos transactions synthétiques en groupes de ressources et appliquer des seuils à chaque transaction synthétique de ce groupe de ressources. Utilisez le gestionnaire de groupes de ressources pour créer un groupe de ressources, et affectez un seuil à ce groupe de ressources. Affectez ensuite un ou plusieurs sous-noeuds de transactions synthétiques à ce groupe de ressources. Le seuil associé au groupe de ressources s'applique désormais à toutes les transactions synthétiques associées.

Procédure

Pour créer un groupe de ressources pour les transactions synthétiques, procédez comme suit :

1. Cliquez sur l'icône **Configuration système** et sélectionnez **Gestionnaire de groupe de ressources**. Créez un groupe de ressources ou éditez un groupe de ressources existant. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 995.

Pour créer un groupe de ressources pour les transactions synthétiques, procédez comme suit :

2. Attribuez un nom et une description à votre groupe de ressources. Dans la table Threshold Assignment, affectez un seuil à votre groupe de ressources, puis cliquez sur **Sauvegarder**. Dans le gestionnaire de groupe de ressources, sélectionnez à nouveau votre groupe de ressources et cliquez sur l'icône **Editer** .
3. Associez votre groupe de ressources aux sous-noeuds de transaction synthétique à partir de la table Affectation de ressource et cliquez sur **Sauvegarder**.

   Le format des sous-noeuds de transaction synthétique est `SO:`*`NomTransaction`*. Par exemple, si l'une de vos transactions se nomme `open_webpage`, le sous-noeud disponible porte le nom `SO:open_webpage`.

Résultats

Vous venez d'organiser vos transactions synthétiques dans un groupe de ressources et d'appliquer un seuil à chaque transaction de ce groupe de ressources.

Création de seuils critiques pour des transactions synthétiques simultanées et échelonnées :

Utilisez le Gestionnaire de seuils pour créer des seuils critiques pour les transactions synthétiques simultanées et échelonnées.

Pourquoi et quand exécuter cette tâche

Créez des seuils qui informent les parties prenantes quand des transactions échelonnées consécutives échouent, ou quand des transactions simultanées échouent sur tous les emplacements de réexécution. Pour plus d'informations, voir «Création et édition d'une transaction synthétique», à la page 1062.

Procédure

Pour créer un seuil critique qui crée un événement quand des instances de réexécution de transaction échelonnée échouent, procédez comme suit :

1. Créez un seuil pour les transactions synthétiques dans le Gestionnaire de seuils. Pour plus d'informations, voir «Création d'un seuil pour les transactions synthétiques», à la page 1068.
2. Dans le Gestionnaire de seuils, sélectionnez **Critique** pour la **Gravité** et entrez 1 minute comme **Intervalle (HHMMSS)** de seuil. Employez la formule suivante pour déterminer les **Echantillons consécutifs requis** :

   Echantillons consécutifs requis = (intervalle de réexécution * échecs consécutifs attendus) - 1

   Par exemple, si l'intervalle de réexécution de la transaction synthétique que vous souhaitez surveiller est de 5 minutes, et que vous souhaitez détecter 8 échecs de réexécution consécutifs, vous devez définir **Echantillons consécutifs requis** sur (5 * 8) - 1 = `39`.
3. Ajoutez une condition. Dans la zone Nouvelle condition, sélectionnez **LOCATION** en tant qu'**Attribut**, sélectionnez **Egal à** en tant qu'**Opérateur** et entrez `Aucun` en tant que **Valeur**. Ajoutez une deuxième condition et définissez **PFAILED** = `100`. Sauvegardez le seuil.
4. Dans la barre de navigation, ouvrez le **Gestionnaire de groupes de ressources**. Créez un groupe de ressources. Affectez une ou plusieurs transactions synthétiques échelonnées à votre groupe de ressources, puis affectez le seuil que vous avez créé dans les étapes 1 à 3 à votre groupe de ressources. Sauvegardez le groupe de ressources. Pour plus d'informations, voir «Création d'un groupe de ressources pour les transactions synthétiques», à la page 1069.

Pour créer un seuil critique qui crée un événement quand des instances de réexécution de transaction simultanée échouent, effectuez les étapes suivantes :

5. Créez un seuil pour les transactions synthétiques dans le Gestionnaire de seuils. Pour plus d'informations, voir «Création d'un seuil pour les transactions synthétiques», à la page 1068.
6. Dans le Gestionnaire de seuils, sélectionnez **Critique** pour la **Gravité** et entrez 1 minute comme **Intervalle (HHMMSS)**. Définissez **Echantillons consécutifs requis** sur la même valeur que l'intervalle de réexécution de la transaction que vous voulez surveiller.

   Par exemple, si l'intervalle de réexécution de la transaction synthétique que vous voulez surveiller est de 5 minutes, définissez **Echantillons consécutifs requis** sur `5`.
7. Ajoutez une condition. Dans la zone Nouvelle condition, sélectionnez **LOCATION** en tant qu'**Attribut**, sélectionnez **Egal à** en tant qu'**Opérateur** et entrez `Aucun` en tant que **Valeur**. Ajoutez une deuxième condition et définissez **PFAILED** = `100`. Sauvegardez le seuil.
8. Créez un groupe de ressources. Affectez une ou plusieurs transactions synthétiques et le nouveau seuil critique à votre groupe de ressources. Pour plus d'informations, voir «Création d'un groupe de ressources pour les transactions synthétiques», à la page 1069.

Résultats

Vous avez créé un seuil critique pour une transaction synthétique échelonnée ou simultanée. Lorsque les conditions de seuil sont remplies, un événement est généré. Vous pouvez surveiller les événements dans l'onglet Evénements du Tableau de bord d'Application Performance.

Instructions pour la maximisation des performances du serveur et des agents dans le cadre de la surveillance des fichiers journaux

Afin de maximiser les performances des agents de système d'exploitation et du serveur Performance Management, vous devez définir les expressions régulières dans le fichier de format (.fmt) et limiter le nombre d'événements de surveillance de fichier journal signalés à la console Cloud APM.

Instructions pour la définition des expressions régulières dans le fichier `.fmt`

Le fichier `.fmt` utilise des expressions régulières qui sollicitent particulièrement l'UC. Afin d'améliorer les performances du serveur et des agents, réduisez au minimum le temps consacré à comparer les enregistrements du journal des sources de surveillance avec les expressions régulières du fichier `.fmt`. Pour cela, suivez les instructions ci-dessous :

Réduisez au minimum l'utilisation des modèles multiligne.

Les modèles multiligne sont onéreux car l'agent doit identifier les enregistrements et déterminer s'ils présentent une correspondance. Lorsque vous utilisez un modèle multiligne représentant une expression régulière contenant le caractère «\n», ou un format de type TEC contenant le jeton '%n', l'agent doit d'abord scinder le fichier surveillé en plusieurs enregistrements de tailles différentes. Puis, il doit comparer les enregistrements aux expressions du fichier de format. Cette procédure implique une double vérification des expressions régulières, ce qui ralentit le traitement. Si vous utilisez un modèle d'une seule ligne, chaque ligne du fichier représente un enregistrement, ce qui accélère le traitement.

Dans certains cas, il est possible d'ignorer certaines lignes, ce qui permet d'obtenir de meilleures performances. Vous trouverez ci-après un exemple d'enregistrement unique d'un journal de trace RAS1 :

```
(4D66DACB.0001-1:RAS1,400,"CTBLD")
+4D66DACB.0001 Component: ira
+4D66DACB.0001 Driver: agent_fac:15/4114877.7
+4D66DACB.0001 Timestamp: Feb 24 2011 13:18:54
+4D66DACB.0001 Target: sos510amdx6-d
```

Ici, pour traiter la ligne :

```
+4D66DACB.0001 Driver: agent_fac:15/4114877.7
```

uniquement, vous pouvez écrire le modèle d'une seule ligne suivant :

```
^\+.*Driver: agent_fac:([0-9\.\/]+)$
```

Ce modèle d'une seule ligne traite la valeur requise sans avoir à recourir au format multiligne. Les quatre autres lignes de l'enregistrement logique sont traitées en tant qu'enregistrements d'une seule ligne qui, parce qu'ils ne présentent aucune correspondance, sont ignorés.

Triez les expressions du fichier de format selon leur fréquence d'occurrence dans le journal de surveillance.

L'agent compare chacun des enregistrements du journal qu'il lit avec les expressions du fichier de format jusqu'à trouver une correspondance. Il commence par la dernière expression du fichier, puis effectue la recherche en remontant. Lorsqu'il trouve une correspondance, il cesse la recherche. Si l'expression la plus consignée est la dernière répertoriée, alors, lorsqu'elle est consignée, elle est la seule expression pour laquelle une comparaison est effectuée.

Si le fichier de format contient 100 expressions, chaque fois qu'un enregistrement de journal correspond à la première expression répertoriée dans le fichier de format, l'agent doit d'abord comparer les 99 autres expressions, ce qui ralentit le traitement. Lorsqu'un enregistrement du journal lu par l'agent ne correspond à aucun des modèles du fichier de format, l'agent doit d'abord le comparer à tous les autres modèles pour savoir qu'il ne correspond pas. Ce processus est long et onéreux.

Incluez autant de données constantes que possible dans les expressions régulières.
Par exemple, si le journal renvoie l'erreur suivante :

```
Disk error on device: /dev/sda1 Disk error on device: /dev/sdb2 yyy
```

vous pouvez écrire cette expression :

```
^Disk.*: .*$
```

Cette expression entraîne une correspondance mais elle force le moteur d'expressions régulières à considérer plus de possibilités sur d'autres lignes qui pourraient être similaires, mais qui finalement ne correspondent pas, par exemple, si le signe : vient à manquer.

Cette expression est plus précise et force le moteur d'expressions régulières à interrompre le traitement des erreurs qui ne présentent aucune correspondance :

```
^Disk error on device: /dev/sd[a-b][0-9]$
```

N'utilisez pas les sous-expressions dont vous n'avez pas besoin.
Les sous-expressions affichées entre parenthèses dans l'exemple qui suit permettent d'informer le moteur d'expressions régulières que vous voulez utiliser une valeur renvoyée dans les données mises en correspondance. Ces sous-expressions impliquent un traitement supplémentaire et ne sont pas nécessaires si vous n'utilisez pas la valeur qui est renvoyée. Par exemple, si le journal renvoie l'erreur suivante :

```
write failure in writing to client 9.27.135.191. Error Broken pipe
```

et que vous incluez l'expression régulière suivante dans le fichier de format, le message d'erreur est capturé à la fin ; mais si vous n'utilisez pas la valeur qui est renvoyée, les performances sont affectées de manière négative :

```
REGEX
WriteFailure

^write failure in writing to client (.*)\. Error
(.*)$

ClientAddr $1
CustomSlot1

END
```

Utilisez des parenthèses dans les expressions à des fins de regroupement.
Vous pouvez utiliser l'opérateur ? afin d'indiquer au moteur d'expressions régulières de ne pas capturer la valeur renvoyée. Ainsi, l'opérateur ? permet de regrouper les valeurs renvoyées uniquement. Ce regroupement affecte les performances de manière positive. Par exemple, si les données de journal suivantes sont renvoyées :

```
Login succeeded on the first attempt for user Bob.
Login succeeded on the third attempt for user Joe.
```

Pour mettre en correspondance les deux valeurs renvoyées, vous devez prendre en compte la première ou la troisième tentative de connexion. Si la tentative de connexion ou l'utilisateur spécifique concernés vous importent peu, vous pouvez inclure cette expression afin de regrouper les valeurs renvoyées :

```
REGEX
LoginSuceeded

^login succeeded on the (?:[a-z]+) attempt for user ([A-Z][a-z]*)\.$

UserName $1
CustomSlot1
END
```

Si possible, évitez d'utiliser l'opérateur OR (|) dans les expressions.

L'opérateur | implique un traitement coûteux. L'opérateur | force le moteur d'expressions régulières à effectuer une sauvegarde et à essayer de mettre en correspondance des valeurs qui ne correspondent pas en temps normal. Une procédure bien plus efficace consiste à utiliser deux expressions distinctes. Prenons par exemple l'expression suivante :

```
REGEX DiskError
^.*disk error.*4|^.*disk failure.*4
END
```

Il est plus judicieux d'utiliser ces deux expressions :

```
REGEX DiskError
^.*disk error.*4
END

REGEX DiskError
^.*disk failure.*4
END
```

Ces expressions renvoient les mêmes résultats.

Important : L'emploi de ces expressions est contraire à l'instruction demandant d'utiliser autant de données constantes que possible, et il s'applique uniquement dans les cas où l'opérateur | est utilisé.

N'utilisez pas d'expressions ambiguës.

Les expressions ambiguës forcent le moteur d'expressions régulières à effectuer des sauvegardes et à rechercher différents moyens de mettre en correspondance une expression. Pour plus d'informations, voir Performance Tips.

Des expressions ambiguës peuvent voir le jour lorsqu'une expression est incluse afin de scinder un long enregistrement en plusieurs sous-expressions. Dans cette version dégénérée de ce problème, l'expression contient un espace entre les deux (.*):

```
(.*) (.*)
```

Dans cet exemple de la version dégénérée, le moteur regex recherche deux chaînes d'expressions (quelles qu'elles soient) séparées par un espace. Toutefois, le caractère * correspondant également à un espace, le moteur d'expressions régulières peut affecter le premier espace qu'il trouve au premier (.*). S'il atteint la fin de l'enregistrement d'entrée sans trouver d'autre espace, il effectue une sauvegarde et lance une nouvelle recherche en utilisant l'espace comme espace littéral appelé dans l'expression.

Pour améliorer les performances, utilisez uniquement des expressions spécifiques. Vous pouvez utiliser l'outil Regex Pal pour vérifier si le fichier de format défini correspond au journal de surveillance. Pour plus d'informations, voir Regex Pal.

Instructions pour limiter les événements de fichier journal signalés

Les instructions suivantes limitent les événements de fichier journal susceptibles d'entraîner de mauvaises performances de la part des agents de système d'exploitation ou du serveur Cloud APM :

Ecrivez les formats spécifiques dans le fichier `.fmt`.

Dans le fichier `.fmt`, écrivez des formats spécifiques capables de renvoyer les enregistrements

appropriés. Par exemple, vous pouvez générer un événement pour une erreur spécifique, par exemple les lignes commençant par `Error:`, et ignorer les lignes commençant par `Warning:`.

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

N'activez pas le paramètre Unmatchlog du fichier `.conf`.

Veillez à ne pas activer le paramètre **Unmatchlog** du fichier `.conf` ; ce paramètre consigne tous les fichiers sans correspondance, surchargeant de ce fait votre système de fichiers.

Indiquez la classe d'événement `*DISCARD*` dans le fichier `.fmt`.

Essayez de limiter l'utilisation de l'UC par l'agent en indiquant la classe d'événement `*DISCARD*` prédéfinie dans le fichier `.fmt` de sorte à supprimer des données intentionnellement. Lorsque vous utilisez la classe d'événement `*DISCARD*`, aucun événement n'est créé pour les enregistrements de journal qui correspondent au modèle du fichier `.fmt`. Par exemple :

```
REGEX *DISCARD*
```

Activez la détection des événements en double sur une plus longue période.

Vous pouvez activer la détection des événements en double à l'aide des clés du fichier `.conf` suivantes :

- DupDetectionKeyAttributes
- EventSummaryInterval
- EventFloodThreshold

Dans cet exemple, les lignes en double sont reconnues par les valeurs *msg* et *CustomSlot1* :

```
DupDetectionKeyAttributes=msg,CustomSlot1
EventSummaryInterval=300
EventFloodThreshold=send_first
```

S'il existe plusieurs événements en double, appliquez les valeurs de seuil *send_first* ou *send_none* aux événements. Pour plus d'informations, voir «Détection et filtrage des événements en double», à la page 1049.

Ecrivez des conditions de seuil spécifiques.

Ecrivez des conditions de seuil spécifiques qui limitent l'ensemble de lignes correspondant au seuil. Par exemple, la formule de seuil suivante entraîne le déclenchement du seuil uniquement lorsqu'un événement de la classe d'événement FileSystemUsage possède une valeur supérieure ou égale à 95 dans CustomInteger1 :

```
( Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Fournissez l'ensemble de fichiers `.conf` et `.fmt` appropriés pour l'agent.

Veillez à fournir l'ensemble de fichiers `.conf` et `.fmt` appropriés pour l'agent. Par exemple, si vous configurez la surveillance du fichier journal pour l'agent de système d'exploitation Windows, veillez à configurer les fichiers `.conf` et `.fmt` spécialement créés pour cet agent.

Interrogez la base de données d'alarmes MongoDB pour déterminer le nombre d'événements ouverts ou le débit d'événements.

- Pour interroger la base de données d'alarmes MongoDB afin de déterminer le nombre d'événements ouverts ou le débit d'événements, procédez comme suit :
  1. Créez un fichier `event-query.js` comportant une requête MongoDB pour la base de données d'alarmes.
     - Cette requête compte tous les événements ouverts et fermés à l'aide du nom de seuil suivant :

       ```
       UDB_DB_Pool_Hit_Rat_Pct_Crit_2 db.alarms.count
       ({"threshold_name" : "UDB_DB_Pool_Hit_Rat_Pct_Crit_2"})
       ```

     - Cette requête compte les événements ouverts et fermés dans MongoDB :

       ```
       db.alarms.count()
       ```

2. Exécutez cette commande afin d'obtenir les résultats de la requête dans le fichier event-query.js : **/opt/ibm/mongodb/bin/mongo 127.0.0.1:27000/alarm -u user -p mongoUsrpasswd@08 <event-count.js**.

- Limitez la quantité d'UC utilisée pour la surveillance du journal. Pour plus d'informations, voir «Variables d'environnement de la surveillance des fichiers journaux», à la page 595.

Administration des composants serveur

Le serveur Cloud APM requiert une maintenance en continu, par exemple, pour modifier les mots de passe et sauvegarder les composants. Utilisez les fonctions disponibles pour les tâches d'administration de serveur. Effectuez ces tâches en tant que superutilisateur.

Mots de passe et ID utilisateur des composants

Divers composants requièrent des ID utilisateur et des mots de passe pour y accéder.

Utilisateurs et mots de passe par défaut

Des ID utilisateur et mots de passe par défaut sont disponibles pour accéder à certains composants.

Le tableau suivant contient une liste des ID utilisateur par défaut, avec l'objet de chaque ID, le mot de passe par défaut de chaque ID utilisateur et le script qui permet de modifier le mot de passe par défaut après l'installation :

Tableau 219. Utilisateurs et mots de passe par défaut

ID utilisateur par défaut	Objet	Mot de passe par défaut	Répertoire et script qui permettent de modifier le mot de passe par défaut après l'installation
gaiandb	Permet d'accéder à la base de données de configuration Derby imbriquée de Cloud APM	gIan08pW0rd	néant
apmadmin	Permet de se connecter à console Cloud APM. L'utilisateur par défaut de Cloud APM est apmadmin. Pour l'information sur la modification de l'utilisateur par défaut, voir «Modification de l'utilisateur apmadmin par défaut», à la page 937.	apmpass	/opt/ibm/ccm/apmpasswd.sh
smadmin	Permet de s'authentifier avec le processus Liberty de server1	apmpass	/opt/ibm/ccm/tools/smapasswd.sh
itmuser	Permet d'accéder au magasin de données de préextraction et aux bases de données SCR et DATAMAR.	db2Usrpasswd@08	/opt/ibm/ccm/db2_users_passwd.sh *nom_utilisateur* Où *nom_utilisateur* est **itmuser**
db2apm db2fenc1 dasusr1	Utilisateurs d'instance Db2	db2Usrpasswd@08	/opt/ibm/ccm/db2_users_passwd.sh *nom_utilisateur* Où *nom_utilisateur* est **db2apm**, **db2fenc1** ou **dasusr1**
admin	Permet d'accéder à la base de données MongoDB, qui stocke les données de suivi des transactions. L'administrateur MongoDB permet de gérer les comptes utilisateur MongoDB et l'utilisateur MongoDB ne possède aucun privilège spécial.	mongoUsrpasswd @08	/opt/ibm/ccm/mongopasswd.sh pour modifier simultanément le mot de passe des deux utilisateurs. Vous êtes invité à saisir l'ancien et le nouveau mot de passe.

Modification d'un mot de passe

Vous pouvez exécuter un script pour modifier le mot de passe des utilisateurs suivants : apmadmin, smadmin, itmuser, db2apm, db2fenc1 et dausr1.

Pourquoi et quand exécuter cette tâche

Le serveur Cloud APM crée un ID utilisateur smadmin avec le mot de passe par défaut apmpass pour les communications entre les composants de Performance Management. Il se peut que vous deviez modifier le mot de passe, par exemple, pour respecter les exigences de sécurité de votre organisation ou si vous avez modifié le mot de passe, mais que vous l'avez oublié lorsque le support IBM vous a demandé d'exécuter l'outil de collecte de données.

Dans Cloud APM, l'utilisateur par défaut est apmadmin. L'utilisateur apmadmin est par défaut membre du rôle Administrateur de rôles.

Si vous modifiez le mot de passe par défaut de l'utilisateur apmadmin lors de l'installation du serveur Cloud APM, le mot de passe de l'utilisateur smadmin est également modifié afin d'utiliser le même mot de passe. Utilisez cette procédure si vous souhaitez que l'utilisateur smadmin utilise un mot de passe différent de celui de l'utilisateur apmadmin ou si vous souhaitez modifier son mot de passe après l'installation du serveur.

Si les bases de données du serveur Cloud APM utilisent un serveur Db2 distant sur un système externe, vous pouvez changer le mot de passe de l'ID utilisateur associé sur ce système. Voir «Modification des mots de passe sur un serveur Db2 distant», à la page 1077.

Procédure

Effectuez la procédure sur le système sur lequel le serveur Cloud APM est installé pour modifier le mot de passe de l'un des ID utilisateur par défaut.

1. Ouvrez le répertoire dans lequel se trouve le script, puis exécutez le script pour le mot de passe à modifier :

Tableau 220. Scripts des mots de passe utilisateur par défaut

ID utilisateur par défaut	Mot de passe par défaut	Répertoire et script du mot de passe à modifier
apmadmin	apmpass	/opt/ibm/ccm/apmpasswd.sh
smadmin	apmpass	/opt/ibm/ccm/tools/smapasswd.sh
itmuser db2apm db2fenc1 dasusr1	db2Usrpasswd@08	/opt/ibm/ccm/db2_users_passwd.sh *nom_utilisateur* Où *nom_utilisateur* est itmuser, db2apm, db2fenc1 ou dasusr1.
admin	mongoUsrpasswd@08	/opt/ibm/ccm/mongopasswd.sh pour modifier simultanément le mot de passe des deux utilisateurs. Vous êtes invité à saisir l'ancien et le nouveau mot de passe.

   Si vous utilisez le script db2_users_passwd.sh lorsque le serveur Db2 se trouve sur le même système que le serveur Cloud APM, le script utilise la commande **passwd** pour changer le mot de passe de l'utilisateur Db2 spécifié et met à jour la configuration du serveur Cloud APM avec le mot de passe modifié.

   Lorsque Cloud APM est configuré pour utiliser un serveur Db2 distant, vous utilisez le script db2_users_passwd.sh de plusieurs manières :

   - Modifiez le mot de passe de l'utilisateur itmuser sur le serveur Cloud APM pour qu'il corresponde à celui qui est défini sur le serveur Db2 distant.

- Modifiez le mot de passe de l'utilisateur `db2apm` sur le système où le serveur Cloud APM est installé.

La configuration du serveur Cloud APM est également mise à jour avec les mots de passe modifiés.

N'utilisez pas le script `db2_users_passwd.sh` pour modifier le mot de passe de l'utilisateur de l'instance Db2 ou les mots de passe de l'utilisateur d'une autre base de données pour le serveur Db2 distant.

Pour modifier le mot de passe de l'utilisateur de l'instance `itmuser` et Db2 lorsque votre configuration utilise un serveur Db2 distant, voir «Modification des mots de passe sur un serveur Db2 distant».

Le serveur Cloud APM est redémarré si vous modifiez le mot de passe pour `itmuser`, mais pas pour les utilisateurs d'une autre base de données.

2. Une fois que vous avez été invité à entrer un nouveau mot de passe, entrez-le, puis appuyez sur Entrée et ressaisissez le nouveau mot de passe lorsque vous y êtes invité.
3. Si vous modifiez le mot de passe `smadmin`, une fois que vous avez été invité à entrer le mot de passe `apmadmin`, entrez-le et appuyez sur Entrée. Le mot de passe `apmadmin` est requis pour mettre à jour la connexion serveur avec le nouveau mot de passe `smadmin`.

Résultats

Le serveur Cloud APM est recyclé et le nouveau mot de passe de l'utilisateur est enregistré.

Tâches associées:

«Modification de l'utilisateur apmadmin par défaut», à la page 937
L'utilisateur par défaut de Cloud APM est apmadmin et le domaine par défaut est customRealm. Par défaut, apmadmin est membre du rôle Administrateur des rôles.

Modification des mots de passe sur un serveur Db2 distant

Si votre serveur Cloud APM utilise un serveur Db2 distant sur un système externe, suivez cette procédure pour changer les mots de passe des utilisateurs Db2 sur le serveur Db2 et configurer le serveur Cloud APM avec le mot de passe `itmuser` mis à jour. Ces étapes diffèrent légèrement de la procédure de modification des mots de passe de l'utilisateur Db2 sur le serveur Cloud APM connecté au serveur Db2 local par défaut.

Pourquoi et quand exécuter cette tâche

Lors de cette procédure, les composants du serveur Cloud APM sont arrêtés. Les composants sont recyclés une fois que vous avez effectué cette procédure.

Procédure

Procédez comme suit en tant que superutilisateur :

1. Arrêtez tous les composants du serveur Cloud APM via la commande suivante :

   ```
   apm stop_all
   ```

2. Sur le système où vous avez installé le serveur Db2, entrez la commande `passwd` suivie du nom de l'utilisateur Db2 dont vous souhaitez changer le mot de passe.
   - Pour l'utilisateur *instance_db2_externe*, entrez `passwd` *`instance_db2_externe`*

     où *instance_db2_externe* est le nom d'utilisateur de l'instance de serveur Db2 distante que vous avez créée lors de la configuration du serveur Db2 distant.
   - Pour l'utilisateur `itmuser`, saisissez `passwd itmuser`
3. Sur le système sur lequel vous avez installé le serveur Cloud APM, exécutez le script `db2_users_passwd.sh` pour changer le mot de passe `itmuser` afin qu'il corresponde à celui que vous avez configuré pour cet utilisateur sur le serveur Db2 distant :

   ```
   rép_install/ccm/db2_users_passwd.sh itmuser
   ```

où *rép_install* se rapporte au répertoire où le serveur serveur Cloud APM est installé. Le répertoire d'installation par défaut est `/opt/ibm`.

Le script `db2_users_passwd.sh` change le mot de passe de l'utilisateur `itmuser` sur le système où le serveur Cloud APM est installé, met à jour la configuration du serveur Cloud APM avec le mot de passe modifié, et redémarre le serveur Cloud APM. Le script ne vérifie pas que le mot de passe peut être utilisé pour la connexion au serveur Db2 distant. Vous devez donc vous assurer que le mot de passe correspond à celui de l'utilisateur `itmuser` sur le serveur Db2 distant.

4. L'utilisateur `db2apm` existe sur le système où vous avez installé le serveur Cloud APM et il est utilisé avec le client Db2 sur ce système. Son mot de passe ne dépend pas de celui de l'utilisateur d'instance Db2 sur le serveur Db2 distant. Si vous devez changer le mot de passe de l'utilisateur `db2apm` sur le serveur Cloud APM, exécutez le script `db2_users_passwd.sh` :

   ```
   rép_install/ccm/db2_users_passwd.sh db2apm
   ```

   Le script `db2_users_passwd.sh` change le mot de passe de l'utilisateur `db2apm` et met à jour le serveur Cloud APM avec le mot de passe modifié. Le serveur Cloud APM n'est pas redémarré lorsque vous changez le mot de passe `db2apm`.

Modification de la version et de l'emplacement du serveur Db2 ou des noms de base de données après l'installation du serveur Cloud APM

Une fois le serveur Cloud APM installé, vous pouvez mettre à niveau votre version locale ou distante du serveur Db2. Vous pouvez également modifier les noms des bases de données Db2 du serveur Cloud APM sur le serveur Db2 distant, modifier le numéro de port, le nom d'hôte ou l'adresse IP du serveur Db2 distant ou déplacer les bases de données du serveur Cloud APM sur un autre système ou vers un utilisateur d'instance Db2 différent.

Tableau 221. Modification des détails Db2

Quelle tâche Db2 souhaitez-vous effectuer ?	Suivez ces étapes
Si vous souhaitez passer d'un serveur Db2 local à un serveur Db2 distant ou que vous souhaitez déplacer les bases de données Db2 du serveur Cloud APM Db2 sur un autre serveur Db2 distant ou vers un utilisateur d'instance Db2 différent, suivez les étapes des rubriques adjacentes. **Remarque :** Les étapes adjacentes couvrent également la modification des noms de base de données Cloud APM ou la modification du mot de passe itmuser lors de la modification des bases de données.	Suivez les étapes des rubriques ci-dessous : 1. «Déplacement des bases de données Db2 vers un autre serveur Db2 ou une instance Db2 différente», à la page 1079. **Remarque :** Lorsque vous déplacez les bases de données Db2 du serveur Cloud APM vers un autre serveur Db2, le nouveau serveur Db2 peut exécuter une version ultérieure de Db2. Par exemple, vous pouvez passer d'un serveur Db2 local, qui exécute Db2 Advanced Enterprise Server Edition version 10.5 à un serveur Db2 distant, qui exécute un groupe de correctifs pris en charge de Db2 Advanced Workgroup Server Edition version 11.1. 2. Catalogage des bases de données Db2 après modification du serveur Db2 3. «Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2», à la page 1087 4. Si vous avez déplacé les bases de données vers un serveur Db2 qui exécute une version ultérieure de Db2, suivez les étapes 1, 4, 5 et 6 de la procédure «Mise à niveau du serveur Db2 vers Db2 Advanced Workgroup Server Edition version 11.1.x», à la page 1089.

Tableau 221. Modification des détails Db2 (suite)

Quelle tâche Db2 souhaitez-vous effectuer ?	Suivez ces étapes
Si vous souhaitez uniquement modifier les noms des bases de données Db2 du serveur Cloud APM, suivez les étapes des rubriques adjacentes.	Effectuez les étapes dans l'ordre suivant : 1. Déconnectez l'activité Db2 du serveur Cloud APM en suivant l'étape 1 de la rubrique «Déplacement des bases de données Db2 vers un autre serveur Db2 ou une instance Db2 différente». 2. Modifiez les noms de base de données en suivant les étapes de la note technique expliquant comment modifier le nom d'une base de données à l'aide de la commande db2relocatedb. 3. Catalogage des bases de données Db2 après modification du serveur Db2 4. «Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2», à la page 1087
Si vous souhaitez modifier uniquement le numéro de port du serveur Db2 et le nom d'hôte ou l'adresse IP du serveur Db2 distant, suivez les étapes des rubriques adjacentes.	Suivez les étapes des rubriques ci-dessous dans l'ordre indiqué : 1. Déconnectez l'activité Db2 du serveur Cloud APM en suivant l'étape 1 de la rubrique «Déplacement des bases de données Db2 vers un autre serveur Db2 ou une instance Db2 différente». 2. Sur le serveur Db2 distant, mettez à jour le numéro de port utilisé par l'instance Db2 ou modifiez l'adresse IP ou le nom d'hôte du serveur Db2 distant. 3. Catalogage des bases de données Db2 après modification du serveur Db2 4. «Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2», à la page 1087
Si vous souhaitez changer les mots de passe des utilisateurs de l'instance itmuser ou db2apm, suivez les étapes de la rubrique adjacente.	Suivez la procédure «Modification d'un mot de passe», à la page 1076.
Si vous souhaitez uniquement mettre à niveau la version du serveur Db2 local ou distant de Db2 Advanced Enterprise Server Edition version 10.5 vers Db2 Advanced Workgroup Server Edition version 11.1.1.	Suivez la procédure «Mise à niveau du serveur Db2 vers Db2 Advanced Workgroup Server Edition version 11.1.x», à la page 1089.

Déplacement des bases de données Db2 vers un autre serveur Db2 ou une instance Db2 différente

Après avoir installé le serveur Cloud APM, vous pouvez déplacer les bases de données Db2 du serveur Cloud APM local vers un serveur Db2 distant ou si vous êtes déjà connecté à un serveur Db2 distant, vous pouvez déplacer les bases de données vers un autre serveur Db2 distant ou vers un utilisateur d'instance Db2 différent.

Pourquoi et quand exécuter cette tâche

Utilisez cette procédure pour sauvegarder et déplacer les bases de données Db2 d'un serveur Db2 local ou distant vers un autre serveur Db2 distant ou vers un utilisateur d'instance Db2 différent. Vous pouvez utiliser les mêmes noms de base de données ou changer les noms de base de données pendant l'opération de déplacement. La procédure suivante utilise la commande Db2 **RESTORE REDIRECT** pour déplacer les bases de données vers le nouveau serveur Db2 distant. Pour déplacer les bases de données, effectuez les tâches principales suivantes :

- Arrêtez le serveur Cloud APM et les connexions aux bases de données Db2 en cours. Pour plus d'informations, voir l'étape 1 décrivant l'arrêt du serveur Cloud APM et des connexions de base de données Db2.
- Sauvegardez les bases de données. Pour plus d'informations, voir l'étape 2 décrivant la sauvegarde des bases de données.
- Déplacez (restaurez) les bases de données Db2 sur le nouveau serveur Db2. Pour plus d'informations, voir l'étape 3 décrivant le déplacement (et la restauration) des bases de données.
- Vérifiez les demandes d'octroi de droits. Pour plus d'informations, voir l'étape 4 décrivant la vérification des demandes d'octroi de droits.
- Configurez TBSMDB pour les fonctions SCR UDF. Pour plus d'informations, voir l'étape 5 décrivant la configuration de TBSMDB pour les fonctions SCR UDF et l'étape 6 décrivant la configuration des fonctions SCR UDF.
- Vérifiez les bases de données. Pour plus d'informations, voir l'étape 7 décrivant la vérification des bases de données.

Lorsque vous suivez les étapes de la procédure ci-après, gardez à l'esprit les éléments suivants :

- Il s'agit d'un exemple de procédure qui explique comment déplacer les bases de données Db2 existantes vers un nouveau serveur Db2. Si l'administrateur Db2 de votre organisation exécute ses propres processus et procédures pour déplacer des bases de données, utilisez les procédures Db2 de votre organisation au lieu de suivre les étapes de cette procédure. Chaque étape de cette procédure est associée à Cloud APM ou à Db2 afin que vous puissiez distinguer les étapes propres à Cloud APM et les étapes propres à Db2.
- Elle inclut les étapes à suivre pour modifier les noms de base de données, le numéro de port, le nom d'instance, le mot de passe et l'emplacement du système de fichiers de la base de données Db2. Si vous souhaitez modifier un élément simple comme le numéro de port Db2, vous pouvez vous reporter aux procédures Db2 standard et exécuter la commande **`db2 update dbm cfg using svcename`** et mettre à jour `/etc/services` au lieu de suivre les étapes ci-dessous pour le numéro de port.
- Les étapes ci-dessous utilisent une sauvegarde hors ligne pour créer les fichiers de sauvegarde. Une fois créés, les fichiers sont copiés sur le nouveau serveur Db2. Sur le nouveau serveur Db2, une commande **`RESTORE REDIRECT`** est utilisée pour créer un script de restauration spécifique. Ce script peut ensuite être utilisé pour déplacer et restaurer les bases de données sur le serveur Db2. Avant son exécution, le script est modifié pour permettre à l'utilisateur d'indiquer un certain nombre d'éléments, comme le répertoire où sont stockées les nouvelles bases de données. Le script exécute le processus de restauration deux fois : une première fois pour effectuer la restauration initiale et une seconde fois avec l'option `CONTINUE` pour traiter les chemins de stockage de groupe de stockage et les conteneurs d'espaces table DMS.

Procédure

Suivez les étapes ci-dessous pour déplacer des bases de données Db2 de Cloud APM vers un nouveau serveur Db2 et éventuellement modifier les noms de base de données par défaut, le numéro de port et l'ID instance.

1. Cloud APM Arrêtez le serveur Cloud APM et les connexions aux bases de données Db2 en cours en suivant les étapes ci-dessous :
   a. En tant que superutilisateur (root), arrêtez le serveur Cloud APM en exécutant la commande suivante :
      ```
      apm stop_all
      ```
   b. Sur le serveur Db2 en cours, exécutez **`su`** pour l'ID utilisateur de l'instance Db2. Par exemple, pour l'ID utilisateur de l'instance `db2apm`, exécutez la commande suivante :
      ```
      su - db2apm
      ```
   c. Démarrez le serveur Db2 en exécutant la commande suivante :
      ```
      db2start
      ```

d. Vérifiez qu'il n'existe pas de connexion à la base de données Db2 de Cloud APM que vous déplacez. Entrez la commande suivante pour vérifier les connexions :

```
db2 list applications
```

Si plusieurs serveur Cloud APM utilisent cette instance Db2, vous pouvez indiquer le nom de la base de données. Par exemple :

```
db2 list applications for db WAREHOUS
```

e. S'il existe des connexions, examinez-les et supprimez-les, si nécessaire, en exécutant la commande suivante :

```
db2 "force application (31441, 54612)"
```

où 31441 et 54612 sont des descripteurs d'application. Vous pouvez utiliser la commande **db2 force applications all** si aucune autre application n'utilise l'instance Db2.

f. Vérifiez une nouvelle fois qu'il n'existe pas de connexion à chacune des bases de données. Par exemple, pour la base de données WAREHOUS, exécutez la commande suivante :

```
db2 list applications for db WAREHOUS
```

où WARESHOUS est la base de données dont vous recherchez les connexions. Une sortie comparable à la sortie ci-dessous est affichée s'il n'existe pas de connexion à cette base de données :

```
SQL1611W  No data was returned by Database System Monitor
```

g. Répétez les étapes 1d, 1e et 1f pour chacune des bases de données.

A l'issue de cette étape, le serveur Db2 est démarré sans connexion aux trois bases de données Db2 déplacées du serveur Cloud APM. Les sauvegardes hors ligne requièrent un répertoire accessible en écriture dont l'ID utilisateur de l'instance Db2 (à savoir l'ID utilisateur par défaut db2apm ou un autre ID utilisateur) est propriétaire ou dans lequel il dispose d'un accès en écriture.

2. Db2 Sauvegardez les bases de données en suivant les étapes ci-dessous.

a. En tant que superutilisateur (root) sur le serveur Db2 en cours, créez un répertoire pour les sauvegardes Db2. Par exemple :

```
mkdir /db2; mkdir /db2/backups/; chown db2apm:db2iadm1 -R  /db2
```

b. A l'aide de l'ID utilisateur de l'instance Db2 sur le serveur DB2 en cours, effectuez une sauvegarde hors ligne pour les trois bases de données Db2 du serveur Cloud APM. Utilisez les noms par défaut WAREHOUS, DATAMART et SCR32 sauf si vos bases de données possèdent des noms différents. Entrez les commandes suivantes :

```
db2 backup db WAREHOUS to /db2/backups/
db2 backup db DATAMART  to /db2/backups/
db2 backup db SCR32 to /db2/backups/
```

Une fois que chaque commande a été exécutée, un fichier de sauvegarde est créé avec un nom comparable au nom /db2/backups/WAREHOUS.0.db2apmc.DBPART000.20180427141206.001 et un message comparable au message ci-dessous s'affiche :

```
Backup successful. The timestamp for this backup image is : 20180727141206
```

The backup file name and output message has a different time stamp to the one in this example.

3. Déplacez (restaurez) les bases de données sur le nouveau serveur Db2 en effectuant les opérations suivantes :

a. Cloud APM Sur le nouveau serveur Db2, vous devez d'abord avoir installé une version prise en charge de Db2 et suivi l'étape 1 et les étapes 2.a à 2k de la rubrique «Connexion à un serveur Db2 distant», à la page 129 pour copier les fichiers du serveur Cloud APM sur le serveur Db2 et créer l'ID utilisateur de l'instance Db2.

b. Cloud APM Si vous souhaitez exécuter la procédure avec le paramètre d'authentification Db2 server_encrypt, suivez l'étape 1 et l'étape 2 dans la rubrique «Modification de l'authentification Db2 de server à server_encrypt», à la page 136.

c. Db2 Suivez les étapes ci-dessous pour les trois bases de données : Copiez la sauvegarde Db2 sur le nouveau serveur Db2, traitez des demandes d'octroi de droits Db2, créez les fichiers `.clp` et restaurez les bases de données Db2 sur le nouveau serveur Db2:

1) Utilisez une commande comme **scp** pour copier les sauvegardes Db2 de l'étape 2.b. sur le nouveau serveur Db2.
2) A l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2 distant, exécutez la commande suivante :

   ```
   db2set DB2_RESTORE_GRANT_ADMIN_AUTHORITIES=ON
   ```

   Remarque : Si le serveur Db2 exécute Db2 Advanced Enterprise Server Edition version 10.5, vous devez également redémarrer le serveur Db2 en exécutant la commande `db2stop` suivie de **db2start** pour activer **db2set update**.
   Vous pouvez également vous connecter à l'aide de l'ID utilisateur précédent de l'instance Db2 et accorder un accès au nouvel ID utilisateur de l'instance après la restauration de chaque base de données.
3) A l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2, exécutez les commandes suivantes pour créer les fichiers `.clp` utilisés ultérieurement dans la procédure.
4) A l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2, exécutez la commande **db2 restore** pour les trois bases de données.

Par exemple :

```
db2set DB2_RESTORE_GRANT_ADMIN_AUTHORITIES=ON
db2 restore db WAREHOUS   from /db2/backups taken at 20180427141206 into WHOUSG
  redirect generate script WHOUSG_db.clp
db2 restore db DATAMART   from /db2/backups taken at 20180427141101 into DMARTG
  redirect generate script DMARTG_db.clp
db2 restore db SCR32  from /db2/backups taken at 20180427141501 into SCRG
  redirect generate script SCRG_db.clp
```

- WAREHOUS, DATAMART et SCR32 sont les noms par défaut des base de données Db2 d'origine.
- `/db2/backups` est le répertoire où les sauvegardes ont été copiées sur le nouveau serveur Db2.
- `20180727141206` est l'horodatage.
- `WHOUSG`, `DMARTG`, et `SCRG` sont les nouveaux noms des bases de données.
- `WHOUSG_db.clp`, `DMARTG_db.clp` et `SCRG_db.clp` sont les noms des fichiers `.clp` de sortie.

Le contenu des fichiers `.clp` apparaît sous la forme suivante :

```
-- ******************************************************************************
-- ** automatically created redirect restore script
-- ******************************************************************************
UPDATE COMMAND OPTIONS USING S ON Z ON DATAMART_NODE0000.out V ON;
SET CLIENT ATTACH_MEMBER  0;
SET CLIENT CONNECT_MEMBER 0;
-- ******************************************************************************
-- ** automatically created redirect restore script
-- ******************************************************************************
RESTORE DATABASE DATAMART
-- USER  <nom_utilisateur>
-- USING '<mot_de_passe>'
FROM '/db2/backups'
TAKEN AT 20180427141101
-- ON '/db2/DATAMART_data'
-- DBPATH ON '<répertoire_cible>'
INTO DMARTG
-- NEWLOGPATH '/db2/DATAMART_data/db2apmc/NODE0000/SQL00001/LOGSTREAM0000/'
-- WITH <nombre_mémoires_tampons> BUFFERS
-- BUFFER <taille_mémoire_tampon>
-- REPLACE HISTORY FILE
-- REPLACE EXISTING
```

```
REDIRECT
-- PARALLELISM <n>
WITHOUT ROLLING FORWARD
-- WITHOUT PROMPTING
```

d. Db2 Modifiez les fichiers `.clp` des trois bases de données. Les informations ci-dessous incluent des instructions pour vous aider à mettre à jour ces fichiers.
   - Les lignes commençant par `--` sont des commentaires.
   - Supprimez la mise en commentaire de la ligne `–ON` et indiquez l'emplacement où vous souhaitez stocker la base de données sur le nouveau serveur Db2. Dans l'exemple précédent, la ligne `ON` était la seule ligne mise à jour de la manière suivante :

     ```
     ON '/db2/db2apmc/WHOUSG_data'
     ```
   - Vous pouvez également supprimer la mise en commentaire de la ligne commençant par `–NEWLOGPATH` pour indiquer l'endroit où les journaux doivent être stockés.
   - Il est inutile de mettre à jour la ligne `–USER` si vous exécutez la restauration à l'aide de l'ID d'instance de l'utilisateur `db2apm` ou à l'aide de votre propre ID d'instance de l'utilisateur Db2.
   - Vous pouvez conserver la mise en commentaire des lignes relatives aux mémoires tampons. Lorsque vous effectuez une opération de restauration, les bases de données Db2 choisissent automatiquement une valeur optimale pour les paramètres **BUFFER**, **buffer size** et **PARALLELISM**.

e. Db2 Pour chaque fichier des trois bases de données, créez le répertoire indiqué par le paramètre dans **ON** dans le fichier `.clp` de la base de données à l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2,. Accédez au répertoire où le fichier `.clp` a été enregistré pour la base de données concernée et exécutez le fichier `.clp`. Voici un exemple pour DMARTG (initialement la base de données DATAMART).

   ```
   mkdir /db2/db2apmc/DMARTG_data
   cd /db2/backups
   db2 -tvf DMARTG_db.clp
   ```

   Le code ci-dessous est un exemple de sortie obtenue après l'exécution du fichier DMARTG `.clp`. Il permet d'exécuter une redirection de la restauration suivie d'une commande **RESTORE DATABASE DATAMART CONTINUE** standard. Il exécute automatiquement la seconde restauration pour traiter le message d'avertissement `SQL1277W` généré lors de la redirection de la restauration. Si la seconde restauration aboutit, le message d'avertissement peut être ignoré.

   ```
   $ db2 -tvf DMARTG_db.clp
   UPDATE COMMAND OPTIONS USING S ON Z ON DATAMART_NODE0000.out V ON
   DB20000I  The UPDATE COMMAND OPTIONS command completed successfully.

   SET CLIENT ATTACH_MEMBER  0
   DB20000I  The SET CLIENT command completed successfully.

   SET CLIENT CONNECT_MEMBER 0
   DB20000I  The SET CLIENT command completed successfully.

   RESTORE DATABASE DATAMART FROM '/db2/backups' TAKEN AT 20180427141101
   ON '/db2/db2apmc/DMARTG_data' INTO DMARTG NEWLOGPATH
   '/db2/db2apmc/DMARTG_data/db2apmg/NODE0000/SQL00001/LOGSTREAM0000/'
   REDIRECT WITHOUT ROLLING FORWARD
   SQL1277W  A redirected restore operation is being performed.
   During a table space restore,
   only table spaces being restored can have their paths reconfigured.
   During a database restore,
   storage group storage paths and DMS table space containers can be reconfigured.
   DB20000I  The RESTORE DATABASE command completed successfully.

   RESTORE DATABASE DATAMART CONTINUE
   DB20000I  The RESTORE DATABASE command completed successfully.
   ```

f. Db2 Si vous effectuez une sauvegarde hors ligne, il est inutile d'exécuter la commande **db2 rollforward**. En revanche, si vous avez des enregistrements de journal en attente, vous devrez

peut-être exécuter les commandes suivantes à l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2 pour pouvoir vous connecter aux bases de données.

```
db2  rollforward db WAREHOUS complete
db2  rollforward db DATAMART complete
db2  rollforward db SCR32 complete
```

où WAREHOUSE, DATAMART et SCR32 sont les noms d'origine des bases de données.

4. Cloud APM Vérifiez les demandes d'octroi de droits. Si vous avez modifié l'ID utilisateur de l'instance Db2 lors du déplacement des bases de données, l'ID utilisateur de l'instance Db2 d'origine peut toujours accéder aux bases de données. Exécutez la commande suivante pour vérifier les octrois de droits existants sur les bases de données. Si l'ID utilisateur de l'instance Db2 dispose d'octrois de droits sur les bases de données, ces octrois de droits doivent être révoqués.

   ```
   db2 connect to nom_bdd
   db2 "SELECT DISTINCT GRANTEETYPE, GRANTEE, SECURITYADMAUTH from SYSCAT.DBAUTH"
   db2 "SELECT DISTINCT GRANTEETYPE, GRANTEE, DBADMAUTH from SYSCAT.DBAUTH"
   db2 connect reset
   ```

   où *nom_bdd* est le nom de l'une des trois bases de données. L'ID utilisateur de l'instance Db2 doit disposer des droits `dbadmin` et `secadm`. L'ID utilisateur itmuser doit disposer des droits `dbadmin`. Les utilisateurs publics doivent disposer des droits `authority=N`. Si d'autres ID sont affichés et disposent de droits, vous souhaitez peut-être les révoquer. La section ci-dessous est un exemple de commande permettant de révoquer les droits.

   ```
   db2 connect to WHOUSG
   db2 REVOKE DBADM ON DATABASE FROM USER db2apm BY ALL
   db2 REVOKE SECADM ON DATABASE FROM USER db2apm BY ALL
   ```

   Dans les commandes précédentes, `db2apm` est l'ID utilisateur par défaut de l'instance Db2. L'ID utilisateur peut être différent si vous l'avez modifié. Suivez cette étape pour les trois bases de données dont vous souhaitez révoquer des droits.

5. Cloud APM Configurez TBSMDB pour les fonctions SCR UDF. Suivez l'étape 2.n de la rubrique «Connexion à un serveur Db2 distant», à la page 129. Lorsque vous suivez l'étape 2.n, répondez à la question `Should the installer create the schema for this database` en indiquant `2` (pour Non) au lieu de 1 (pour Oui), comme décrit à l'étape 2.n.

6. Cloud APM Configurez les fonctions SCR UDF. Installez les fichiers jar et créez les fonctions UDF. Suivez cette étape une fois pour chaque instance Db2. Les fichiers `*_JAR.jar` sont installés dans le répertoire *répertoire_base_instance_Db2*`/sqllib/function/jar/TBSMUDF`. Exécutez les commandes suivantes à l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2.

   ```
   cd $home
   cd tbsmdb/sql
   db2 connect to nom_bdd
   db2 -v -f ./tbsmudf_cleanupudf.db2.sql -t
   db2 -v -f ./tbsmudf_removeudf.db2.sql -t
   db2 -v -f ./tbsmudf_installudf.db2.sql -t
   db2 -v -f ./tbsmudf_setupudf.db2.sql -t
   db2 connect reset
   ```

   où *nom_bdd* est le nom de l'une des trois bases de données. S'il s'agit de la première base de données ajoutée à l'instance Db2, des messages d'erreur risquent de s'afficher lorsque vous exécutez les commandes SQL **`cleanupudf`** et **`removeudf`**. Ignorez les messages et exécutez les commandes SQL **`installudf`** et **`setupudf`** restantes.

7. Vérifiez les bases de données. A l'aide de l'ID utilisateur de l'instance Db2 sur le nouveau serveur Db2 distant, connectez-vous à la base de données SCR et exécutez la commande select. Par exemple :

   ```
   db2 connect to scr32;
   db2 "select ROUTINE_CATALOG, ROUTINE_SCHEMA, ROUTINE_NAME, ROUTINE_TYPE from sysibm.routines "
   | grep -i TBSMUDF |wc -l
   ```

   Le nombre de lignes doit correspondre à 32 fonctions environ.

Résultats

Les trois bases de données sont déplacées vers le nouveau serveur Db2, l'ID utilisateur de l'instance Db2 que les bases de données utilisent est changé et les fonctions de Cloud APM sont ajoutées à la base de données SCR.

Que faire ensuite

«Catalogage des bases de données Db2 après modification du serveur Db2».

Catalogage des bases de données Db2 après modification du serveur Db2

Si vous modifiez le nom des bases de données Db2, le noeud du serveur Db2 ou le numéro de port Db2, vous devez mettre à jour les catalogues.

Pourquoi et quand exécuter cette tâche

Lorsque vous cataloguez une base de données, vous pouvez attribuer à *authentification* la valeur `server` ou `server_encrypt` en fonction de la configuration de l'authentification sur le serveur Db2. Pour plus d'informations, voir «Modification de l'authentification Db2 de server à server_encrypt», à la page 136. L'exemple suivant montre comment définir l'authentification sur `server_encrypt` pour le noeud du serveur Db2 `APMG` lorsque vous cataloguez la base de données `DMARTG`.

```
db2 catalog database DMARTG as DATAMART at node APMG authentication server encrypt
```

Remarque : Si vous ne modifiez le noeud du serveur Db2 ou le numéro de port Db2 qu'au moment de déplacer les bases de données Db2 d'un serveur Db2 à un autre serveur Db2, vous devez uniquement recataloguer le noeud du serveur Db2. Entrez les commandes suivantes :

1. Pour décataloguer le noeud, entrez la commande suivante :

   ```
   db2 uncatalog node noeud_serveur_Db2
   ```

   où *noeud_serveur_Db2* correspond au noeud du serveur Db2 existant.
2. Cataloguez le nouveau serveur Db2. Entrez la commande suivante :

   ```
   db2 catalog tcpip node noeud_serveur_Db2_actuel remote
    nouveau_serveur_Db2 server nouveau_port_db2
   ```

   où :

   - *noeud_serveur_Db2_actuel* correspond au noeud du serveur Db2 actuel.
   - *nouveau_serveur_Db2* correspond au nom d'hôte ou à l'adresse IP du nouveau serveur Db2.
   - *port_db2* correspond au nouveau numéro de port Db2.

   Vous pouvez éventuellement définir le type d'authentification au moment d'entrer la commande **db2 catalog**. Vous devez décataloguer et recataloguer le noeud `APM_NODE` qui a été créé lors de l'installation initiale du serveur Cloud APM, puis décataloguer et recataloguer tous les noeuds supplémentaires que vous avez créés.

   Pour plus d'informations sur les commandes **db2 catalog tcpip node**, voir Commande CATALOG TCPIP/TCPIP4/TCPIP6 NODE. Pour plus d'informations sur la commande **db2 catalog db**, voir Commande CATALOG DATABASE.

Procédure

Pour cataloguer les bases de données, les noeuds du serveur Db2 et le numéro de port Db2, procédez comme suit :

Remarque : Il s'agit d'un exemple de procédure. Les commandes du catalogue que vous utilisez pour effectuer votre catalogage seront les mêmes, mais le nom des bases de données, le noeud du serveur Db2, le nom d'hôte du serveur Db2, le numéro de port et le mot de passe itmuser seront différents.

1. Sur le serveur Cloud APM, entrez **su** dans l'ID de l'utilisateur d'instance Db2. Par exemple, pour l'ID de l'utilisateur d'instance db2apm, entrez la commande suivante :

   ```
   su - db2apm
   ```

2. Exécutez les commandes **catalog** suivantes pour cataloguer les bases de données, le noeud du serveur Db2 et le numéro de port Db2.

   a. Sauvegardez une copie des informations de votre catalogue actuel. Par exemple :

   ```
   db2 list db directory  >> /tmp/db.directory
   db2 list node directory >> /tmp/node.directory
   ```

   b. Décataloguez le noeud du serveur Db2 existant. Entrez la commande suivante :

   ```
   db2 uncatalog node noeud_serveur_Db2
   ```

   c. Cataloguez le nouveau noeud du serveur Db2. Entrez la commande suivante :

   ```
   db2 CATALOG TCPIP NODE nouveau_noeud REMOTE serveur_db2 SERVER port_db2
   ```

   où *nouveau_noeud* est APMG, *serveur_db2* est db21056.rtp.raleigh.ibm.com et *port_db2* est 50005.

   d. Décataloguez les bases de données d'origine par défaut. Entrez les commandes suivantes :

   ```
   db2 uncatalog db WAREHOUS
   db2 uncatalog db DATAMART
   db2 uncatalog db SCR32
   ```

   e. Cataloguez vos nouvelles bases de données comme noms des nouvelles bases de données par défaut. Entrez les commandes suivantes :

   ```
   db2 catalog db nouvel_entrepôt at node nouveau_noeud
   db2 catalog db nouvel_entrepôt_données at node nouveau_noeud
   db2 catalog db nouveau_scr32 at node nouveau_noeud
   ```

   où *nouvel_entrepôt* est WHOUSG, *nouvel_entrepôt_données* est DMARTG, *nouveau_scr32* est SCRG et *nouveau_noeud* est APMG. N'utilisez jamais APM_NODE comme nom de poste car le serveur Cloud APM utilise déjà le nom de poste APM_NODE.

   Le type de sortie suivant s'affiche lorsque les commandes de catalogue s'exécutent.

   ```
   DB2XXXX  The CATALOG X command completed successfully.
   ```

   f. Cataloguez les noms d'alias par défaut pour les nouvelles bases de données. Entrez les commandes suivantes :

   ```
   db2 catalog db nouvel_entrepôt as WAREHOUS at node nouveau_noeud
   db2 catalog db nouvel_entrepôt_données as DATAMART at node nouvel_entrepôt_données
   db2 catalog db nouveau_scr32 as SCR32 at node nouveau_noeud
   db2 terminate
   ```

   g. Testez les connexions aux nouvelles bases de données. Entrez les commandes suivantes :

   ```
   db2 connect to nouvel_entrepôt user itmuser using mdp_itm
   db2 connect to nouvel_entrepôt_données user itmuser using mdp_itm
   db2 connect to nouveau_scr32 user itmuser using mdp_itm
   db2 connect to WAREHOUS user itmuser using mdp_itm
   db2 connect to DATAMART user itmuser using mdp_itm
   db2 connect to SCR32 user itmuser using mdp_itm
   db2 terminate
   ```

   En fonction des variables, *mdp_itm* est xxxyyy dans les commandes précédentes. Une sortie semblable à la suivante s'affiche si les connexions sont réussies : Cette sortie correspond à la nouvelle base de données DMARTG.

   ```
   $ db2 connect to nouvel_entrepôt_données user itmuser using mdp_itm
   Database Connection Information

   Database server        = DB2/LINUXX8664 10.5.6
   SQL authorization ID   = ITMUSER
   Local database alias   = DMARTG
   ```

Résultats

Les nouvelles bases de données, le noeud du serveur Db2 et le numéro de port sont catalogués.

Que faire ensuite

«Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2»

Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2

Si vous passez à un serveur Db2 différent, à un utilisateur d'instance Db2 différent, ou si vous modifiez le nom d'hôte, l'adresse IP ou le numéro de port du serveur Db2, ou les noms des bases de données Db2, vous devez reconfigurer le serveur Cloud APM pour qu'il prenne en compte les modifications du serveur Db2.

Avant de commencer

Avant de mettre à jour la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2, vous devez recataloguer les bases de données Db2 sur votre serveur Cloud APM pour l'ID utilisateur de l'instance Db2 que vous utilisez. Si cette tâche n'est pas terminée, voir «Catalogage des bases de données Db2 après modification du serveur Db2», à la page 1085 pour obtenir les instructions à suivre pour continuer la procédure.

Pourquoi et quand exécuter cette tâche

Si vous déplacez les bases de données Db2 d'un serveur Db2 à un autre, ou si vous modifiez les noms des bases de données, l'ID utilisateur de l'instance Db2 ou le numéro de port, vous devez reconfigurer le serveur Cloud APM pour qu'il prenne en compte les modifications de base de données en utilisant le script `update_db_config.sh`.

Pour accéder au script `update_db_config.sh`, vous devez installer le correctif temporaire 6 ou ultérieur d'IBM Cloud Application Performance Management Private, V8.1.4.0 (`8.1.4.0-IBM-APM-SERVER-IF0006`) après avoir terminé l'installation du serveur Cloud APM. Les correctifs temporaires pour le serveur Cloud APM version 8.1.4 peuvent être téléchargés à partir d'IBM Fix Central. Une fois le correctif temporaire installé, le script `update_db_config.sh` est placé sous le répertoire *`rép_install`*`/ccm/`. *rép_install* est le répertoire dans lequel vous avez installé votre serveur Cloud APM.

Les étapes de cette procédure utilisent le répertoire `/opt/ibm` par défaut en tant que répertoire d'installation du serveur Cloud APM. Si vous avez spécifié un répertoire différent lors de l'installation du serveur, utilisez-le à la place de `/opt/ibm` dans les étapes suivantes.

Le mot de passe de l'utilisateur itmuser sur le serveur Cloud APM est changé pour correspondre à celui défini sur votre nouvelle base de données distante au cours de cette procédure. Le serveur Cloud APM est redémarré lors de l'exécution du script `update_db_config.sh`.

Procédure

Suivez les étapes ci-dessous pour reconfigurer le serveur Cloud APM pour qu'il corresponde aux modifications de la nouvelle base de données.

1. Sous l'ID utilisateur de l'instance Db2, connectez-vous au nouveau serveur Db2 et démarrez Db2 s'il n'est pas déjà en cours d'exécution. Lancez la commande suivante :
   ```
   db2start
   ```
2. En tant que superutilisateur, connectez-vous au serveur Cloud APM et démarrez les services Cloud APM qui sont peut-être arrêtés. Lancez la commande suivante :
   ```
   apm start_all
   ```
3. En tant que superutilisateur, exécutez le script `/opt/ibm/ccm/update_db_config.sh` avec les paramètres de configuration et les valeurs associées qui correspondent au nouveau serveur Db2. Veillez à entrer correctement les valeurs de tous les paramètres de configuration car le script `update_db_config.sh`

met à jour les fichiers de configuration pour les trois bases de données même si vous modifiez la configuration de l'une d'entre elles uniquement. Les paramètres de configuration sont les suivants :

- `-h` **`rép_install`** est le répertoire dans lequel le serveur Cloud APM est installé. Le répertoire d'installation par défaut est `/opt/ibm`.
- `-server` **`nomhôte_ou_adresseip`** est l'emplacement du répertoire et le nom d'hôte ou l'adresse IP du nouveau serveur Db2.
- **`-db2_port`** est le nouveau numéro de port Db2.
- **`-whous_db`** est le nom de votre base de données WAREHOUS. Le nom par défaut est WAREHOUS. Si vous utilisez un nouveau nom à la place du nom par défaut, entrez le nouveau nom.
- **`-scr_db`** est le nom de votre base de données SCR32. Le nom par défaut est SCR32. Si vous utilisez un nouveau nom à la place du nom par défaut, entrez le nouveau nom.
- **`-dm_db`** est le nom de votre base de données DATAMART. Le nom par défaut est DATAMART. Si vous utilisez un nouveau nom à la place du nom par défaut, entrez le nouveau nom.
- **`-db2_inst`** est le nouvel ID d'instance de l'utilisateur Db2. L'ID utilisateur par défaut est `db2apm`.
- **`db_pw`** est le mot de passe itmuser sur le système où le serveur Db2 est installé.

Exemple d'exécution de `update_db_config.sh` :

```
./update_db_config.sh -h /opt/ibm -server db21056.rtp.raleigh.ibm.com -db2_port 50005
 -scr_db SCRG -dm_db DMARTG -whous_db WHOUSG -db2_inst db2apmg -db_pw xxxyyy
```

Si vous n'entrez pas le mot de passe itmuser sur la ligne de commande avec les autres paramètres de configuration, vous êtes invité à l'indiquer.

4. Démarrez Cloud APM. Lancez la commande suivante :

   ```
   apm restart_all
   ```

5. Effectuez une sauvegarde sur le serveur Cloud APM. Pour plus d'informations, voir «Sauvegarde des composants», à la page 1104.

Résultats

Le serveur Cloud APM est reconfiguré pour utiliser les informations de la nouvelle connexion de base de données.

Que faire ensuite

Si d'autres produits utilisent ces bases de données, mettez à jour leur configuration. Par exemple, si vous modifiez le nom d'hôte, l'adresse IP ou les noms des bases de données du serveur Db2 Cloud APM et que vous avez précédemment intégré ce dernier à d'autres produits tels que Tivoli Common Reporting, procédez comme suit :

1. Décataloguez le noeud et les bases de données d'origine du serveur Db2 sur le serveur Tivoli Common Reporting. Lancez les commandes suivantes :

   ```
   db2 list node directory >> répertoire_noeud_serveur_db2
   db2 uncatalog node noeud_serveur_db2_d'origine
   db2 list db directory >> répertoire_db2
   db2 uncatalog db nom_bd_d'origine
   ```

   où :

   - *répertoire_noeud_serveur_db2* est le répertoire de noeud du serveur Db2 d'origine.
   - *noeud_serveur_db2_d'origine* est le noeud du serveur Db2 d'origine.
   - *répertoire_db2* est le répertoire Db2 d'origine.
   - *nom_bd_d'origine* est le nom de base de données d'origine.

2. Recataloguez les nouvelles bases de données du serveur Db2 sur le serveur Tivoli Common Reporting en suivant les étapes décrites dans la rubrique «Configuration d'une connexion ODBC», à la page 918.

3. Reconfigurez et réinstallez les rapports pour mettre à jour la connexion Tivoli Data Warehouse et APPMART en suivant les étapes décrites dans la rubrique «Configuration de l'image d'installation des rapports», à la page 919.

Connectez-vous à la console Cloud APM et vérifiez que vos agents peuvent se connecter au serveur Cloud APM.

Mise à niveau du serveur Db2 vers Db2 Advanced Workgroup Server Edition version 11.1.x

Une fois le serveur Cloud APM installé, vous pouvez mettre à niveau votre serveur Db2 local ou distant de Db2 Advanced Enterprise Server Edition version 10.5 vers Db2 Advanced Workgroup Server Edition version 11.1.x

Pour la liste des versions Db2 11.1 prises en charge, utilisez les liens contenus dans la section Product reports du document System requirements (APM Developer Center). Lorsque le rapport de compatibilité des produits logiciels s'affiche, cliquez sur l'onglet **Prerequisites** pour afficher les exigences de la base de données.

Avant de commencer

Assurez-vous que le correctif temporaire 4 ou ultérieur d'IBM Cloud Application Performance Management, Private V8.1.4.0 est appliqué au serveur Cloud APM. Les correctifs temporaires du serveur Cloud APM V8.1.4 peuvent être téléchargés à partir d'IBM Fix Central.

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau le serveur Db2, suivez les instructions qui s'appliquent au serveur Db2 dans IBM Db2 Version 11.1 Knowledge Center. Suivez ensuite des étapes supplémentaires afin de mettre à jour le serveur Db2 pour utiliser les fichiers jar du serveur Cloud APM et mettre à niveau le client Db2 sur le serveur Cloud APM.

Procédure

Suivez la procédure sur le serveur Cloud APM et sur le serveur Db2 si ce dernier est distant.

1. Sur le système où le serveur Cloud APM est installé, arrêtez tous les composants du serveur en exécutant la commande suivante dans le répertoire `/usr/bin` :

   ```
   apm stop_all
   ```

2. Sur le système où le serveur Db2 est installé, mettez à niveau le serveur Db2 en suivant les instructions appropriées dans IBM Db2 Version 11.1 Knowledge Center.
3. Sur le système où le serveur Db2 est installé, configurez la nouvelle version de Db2 pour utiliser les fichiers jar du serveur Cloud APM en exécutant les étapes suivantes :
   a. Entrez la commande Db2 suivante à partir d'une fenêtre de commande Db2

      ```
      db2 connect to bd-scr user utilisateur-instance-db2 using motdepasse-instance-db2
      ```

      Où :
      - *bd-scr* est le nom de la base de données SCR. La valeur par défaut est `SCR32`.
      - *utilisateur_instance-db2* est l'utilisateur de l'instance Db2. La valeur par défaut est `db2apm`.
      - *motdepasse-instance-db2* est le mot de passe de l'utilisateur de 'instance Db2. La valeur par défaut est `db2Usrpasswd@08`.

   b. Accédez à l'un des répertoires suivants :
      - serveur Db2 local :

        ```
        cd rép_install/db2/tbsmdb/sql
        ```

      - serveur Db2 distant :

```
cd chemin-spécifié-dans-setup-db-config/sql
```

où *chemin-spécifié-dans-setup-db-config* est le chemin d'accès que vous avez indiqué pour l'instance Db2 lors de l'exécution du programme **setup-dbconfg** de Cloud APM. Le chemin par défaut est `/opt/IBM/tivoli/tbsmdb`.

c. Exécutez les fichiers `.sql` suivants :

```
db2 -vf ./tbsmudf_cleanupudf.db2.sql -t
db2 -vf ./tbsmudf_removeudf.db2.sql -t
db2 -vf ./tbsmudf_installudf.db2.sql -t
db2 -vf ./tbsmudf_setupudf.db2.sql -t
```

d. Exécutez la commande suivante :

```
db2 connect reset
```

4. Sur le système où le serveur Cloud APM est installé, mettez à niveau le composant IBM Data Server Client à partir du module d'installation Db2 pour qu'il corresponde à la version du serveur Db2. Suivez les instructions dans IBM Db2 Version 11.1 Knowledge Center.
5. Sur le système où le serveur Cloud APM est installé, vérifiez que la variable *KQZ_JDBC_JAR_PATHS* est définie sur le chemin où se trouve le pilote JDBC du client Db2 mis à niveau. Pour mettre à jour la variable *KQZ_JDBC_JAR_PATHS*, procédez comme suit :
   a. Accédez au répertoire *rép_install*`/serveragents/config`.
   b. Sauvegardez le fichier *nomhôte*`_te.cfg`, où *nomhôte* est le nom d'hôte du serveur Cloud APM.
   c. Ouvrez le fichier *nomhôte*`_te.cfg` et recherchez la ligne suivante qui commence par `KQZ_JDBC_JAR_PATHS=`.
   d. Définissez la valeur *KQZ_JDBC_JAR_PATHS* sur le chemin où se trouvent les fichiers jar du pilote JDBC Db2 V11.1.

      Par exemple, si vous utilisez Db2 V11.1 et qu'IBM Data Server Client est installé dans le répertoire `/opt/ibm` par défaut, le chemin *KQZ_JDBC_JAR_PATHS* est similaire à celui-ci : `KQZ_JDBC_JAR_PATHS=/opt/ibm/db2/V11.1/java`.
   e. Sauvegardez et fermez le fichier.
6. Démarrez tous les composants de serveur en exécutant la commande suivante dans le répertoire `/usr/bin` :

```
apm start_all
```

Résultats

Votre serveur Db2 auquel le serveur Cloud APM est connecté est mis à niveau.

A faire : Si vous effectuez une sauvegarde et une restauration pour une reprise après incident, veillez à mettre à niveau le serveur Db2 afin qu'il corresponde à la version utilisée par le serveur source avant de terminer la restauration sur le serveur cible.

Démarrage, arrêt et vérification du statut des composants serveur

Utilisez les commandes de vérification du statut, de démarrage, d'arrêt et de recyclage des composants du serveur Cloud APM lorsque cela est nécessaire pour les tâches de maintenance et d'identification et de résolution des problèmes.

Pourquoi et quand exécuter cette tâche

En tant que superutilisateur, exécutez l'une des commandes **apm** dans le répertoire `/usr/bin/` sur le système sur lequel le serveur Cloud APM est installé. Une version abrégée de chaque commande est disponible et affichée sous le libellé «Commande abrégée».

Procédure

En tant que superutilisateur, effectuez l'une des étapes suivantes :

- Pour répertorier les commandes disponibles et en afficher la syntaxe, entrez la commande suivante :

  ```
  apm --help
  ```

- Pour démarrer, arrêter ou recycler tous les composants serveur, entrez l'une des commandes suivantes :

  ```
  apm start_all
  apm stop_all
  apm restart_all
  ```

  Commandes abrégées : **sta**, **spa** et **rta**

- Pour vérifier si tous les composants Cloud APM ou un composant en particulier est en cours d'exécution ou arrêté, saisissez l'une des commandes suivantes :

  ```
  apm status
  ```

  pour tous les composants.

  ```
  apm status nom_composant
  ```

  où *nom_composant* est le nom de l'un des composants suivants.

Option	Description
apmui	Composant de console Cloud APM qui gère les demandes entrantes de l'interface utilisateur.
biagent	Composant pour les collecteurs de données Cloud APM, activé par défaut.
db2	Serveur Db2 utilisé pour conserver les données de surveillance et les applications affichées dans la console Performance Management. Ce composant est utilisé seulement si vous installez un serveur Db2 local avec le serveur Cloud APM.
dqe	Composant pour les collecteurs de données Cloud APM, activé par défaut.
kafka	Composant du bus de messages pour les communications internes entre les composants.
ksy	Agent Summarization and Pruning permettant de gérer les partitions de base de données et d'élaguer les données de surveillance sur le serveur Db2.
min	Composant Noeud d'infrastructure de surveillance qui gère la liste des agents connectés, les données de configuration avancées et les événements de seuil. Ce composant est également le composant de l'interface des agents qui inclut l'interface REST des agents et le serveur HTTP de Central Configuration Services. L'interface REST permet aux agents d'envoyer les données de surveillance conservées dans le serveur Db2 et les événements de seuil. Le serveur HTTP de Central Configuration Services gère les demandes des agents pour les fichiers de configuration. Par exemple, les définitions de seuil.

Option	Description
mongodb	(indisponible avec Cloud APM, Base Private) La base de données open source MongoDB NoSQL qui stocke les données pour les événements de seuil et pour la fonction de suivi des transactions. Ce composant est utilisé seulement si vous installez une base de données MongoDB locale avec le serveur Cloud APM.
oidc	OpenID Connect (OIDC) est un protocole d'identité simple sur OAuth 2.0. Le fournisseur OIDC dans le profil Liberty est implémenté en tant qu'extension OAuth 2.0.
oslc	Fournisseur de services Open Services for Lifecycle Collaboration qui enregistre les ressources des systèmes informatiques, des serveurs de logiciels et des applications surveillées par les agents dans le registre des composants de service.
scr	Registre des composants de service qui conserve les définitions d'application et leurs relations avec les ressources d'agent sur le serveur Db2.
server1	Composant back end de la console Cloud APM qui extrait les données de surveillance et les applications du serveur Db2 et conserve les définitions de seuil, les définitions de groupe de ressources et les définitions de contrôle d'accès basé sur les rôles. Sachez que si vous redémarrez server1, vous devez également redémarrer le composant apmui après avoir redémarré le composant server1.
soagent	(Non disponible avecCloud APM, Base Private) Agent qui agrège les données de transaction de multiples agents de diffusion et génère des événements selon les définitions de seuil. Sachez que si vous arrêtez ce composant, l'agent ne peut pas générer d'événements.
spark	(Non disponible avec Cloud APM, Base Private) Composant qui contrôle l'infrastructure du service spark et les applications, telles AAR Aggregator et Instance Analyzer, qui fonctionnent dessus. Si vous arrêtez ce service, la fonctionnalité est perdue.
txagent	(Indisponible avec Cloud APM, Base Private) Agent d'événement de transactions qui définit les seuils utilisés pour classifier les transactions de middleware. Si vous arrêtez ce composant, la fonctionnalité est perdue.
uview	Service Vue universelle permettant de définir les pages de tableau de bord dans l'onglet Vues personnalisées du Tableau de bord d'Application Performance.

Commande abrégée : **ss**

- Si le support IBM ou une rubrique d'IBM Knowledge Center vous a demandé de démarrer, d'arrêter ou de redémarrer un composant particulier, entrez la commande à l'aide de la syntaxe suivante :

  apm *commande nom_composant*

  , *commande* correspondant à l'une des commandes **apm** suivantes :

Option	Description
start	Lance le *nom_composant* indiqué. Commande abrégée : **st**.

Option	Description
stop	Arrête le *nom_composant* indiqué. Pour un arrêt forcé, insérez **-f** ou **--force** entre **apm** et **stop**. Par exemple, la commande `apm -f stop apmui` arrête immédiatement console Cloud APM. Commande abrégée : **sp**
restart	Redémarre le *nom_composant* en cours d'exécution. Sachez qu'après avoir redémarré le composant server1, vous devez également redémarrer le composant `apmui`. Commande abrégée : **rt**

où *nom_composant* correspond à l'un des composants répertoriés à l'étape précédente (apmui, biagent, db2, dqe, kafka, ksy, min, mongodb, oidc, oslc, scr, server1, soagent, spark ou txagent).

Remarque : Si le message suivant est affiché une fois que vous avez démarré ou arrêté un composant :

```
Ce processus exécute actuellement des opérations de démarrage/arrêt du composant
nom_composant: ID_processus. Attendez qu'il se termine, puis renouvelez l'opération.
```

Cela signifie que le service spécifique est déjà démarré ou arrêté par la commande **apm** exécutée sous l'ID processus affiché. Pour vérifier le statut de ce service, exécutez la commande

```
apm status nom_service
```

. Si le service est toujours exécuté par l'intermédiaire de la commande **apm**, attendez quelques minutes qu'il se termine, puis réessayez l'opération.

Remarque : Si un service ne s'arrête pas lorsque vous utilisez la commande `apm stop nom_service`, `apm stop_all`, ou `apm restart_all`, n'utilisez pas la commande **kill** de Linux pour arrêter le processus. Utilisez plutôt l'option **-f** ou **--force** avec la commande `apm stop nom_service` pour arrêter le processus. L'option -f ou --force doit être utilisée seulement lorsque vous ne pouvez pas arrêter le processus normalement.

Gestion de la taille du segment de mémoire Java maximale et du pool de mémoire tampon Db2

Gérez la taille de segment de mémoire Java maximale et du pool de mémoire tampon Db2 à l'aide de la commande **server_size.sh**.

Procédure

1. Pour afficher la taille du serveur, exécutez la commande **server_size.sh** à partir du répertoire `/opt/ibm/ccm/`. La sortie décrit le nombre d'UC, la taille de mémoire et l'espace disque disponible sur le serveur. Une taille de serveur recommandée est indiquée en fonction de ces informations :

   ```
   Nombre d'UC : 6
   Taille de mémoire : 16 Go
   Taille de serveur recommandée : petite
   Taille de serveur en cours : moyenne
   ```

2. Pour modifier la taille du serveur et le pool de mémoire tampon Db2, exécutez de nouveau la commande **server_size.sh**, suivie de la taille recommandée. Par exemple, **server_size.sh small**. Notez que cette commande arrête et redémarre les quatre serveurs Liberty. La taille du segment de mémoire Java maximale est ajustée en fonction des valeurs indiquées dans le tableau suivant :

Tableau 222. Paramètre de taille de segment de mémoire Java

serveur Cloud APM, composants	Petite	Moyenne	Grande
Serveur d'applications server1	1536 Mo	2048 Mo	3072 Mo

Tableau 222. Paramètre de taille de segment de mémoire Java (suite)

serveur Cloud APM, composants	Petite	Moyenne	Grande
Service APMUI	1536 Mo	3072 Mo	4096 Mo
Uviews (instance de serveur Liberty)	1024 Mo	1024 Mo	1024 Mo
MIN (instance de serveur Liberty)	512 Mo	1536 Mo	2048 Mo
OIDC	128 Mo	128 Mo	256 Mo
Kafka	256 Mo	512 Mo	512 Mo
Zookeeper	256 Mo	256 Mo	256 Mo
MongoDB Cache	1024 Mo	2048 Mo	4096 Mo

Le pool de mémoire tampon est ajusté en fonction des valeurs indiquées dans le tableau suivant :

Tableau 223. Pool de mémoire tampon Db2

Base de données	Pool de mémoire tampon	Grande	Moyenne	Petite
DATAMART	IBMDEFAULTBP	200000	100000	50000
WAREHOUS	IBMDEFAULTBP	300000	200000	100000
SCR32	TBSMSCR16KBP	100000	50000	30000
SCR32	TBSMCFG16KBP	10000	5000	1000

Voici un exemple de sortie :

```
/opt/ibm/ccm/server_size.sh small

Setting heap size to 256 MB for service kafka.
Setting heap size to 256 MB for service zookeeper.
Setting heap size to 1024 MB for service apmui.
Setting heap size to 512 MB for service min.
Setting heap size to 128 MB for service oidc.
Setting heap size to 1526 MB for service server1.
Setting ENABLE_MY_COMPONENTS to true for service apmui.
Setting cache size (GB) to 1 for service mongodb.
Setting prefetch pause to 100000 for service min.
Setting prefetch resume to 75000 for service min.
Setting datamart_ibm_default_buf_pool value to 100.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = DATAMART

DB20000I  The SQL command completed successfully.
Setting scr_ibm_default_buf_pool value to 5000.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = SCR32

DB20000I  The SQL command completed successfully.
Setting scr_tbsm_cfg_16k_buf_pool value to 1000.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
```

```
 SQL authorization ID   = DB2APM
 Local database alias   = SCR32

DB20000I  The SQL command completed successfully.
Setting scr_tbsm_4k_buf_pool value to 1000.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = SCR32

DB20000I  The SQL command completed successfully.
Setting scr_tbsm_scr_16k_buf_pool value to 30000.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = SCR32

DB20000I  The SQL command completed successfully.
Setting scr_tbsm_32k_buf_pool value to 1000.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = SCR32

DB20000I  The SQL command completed successfully.
Setting scr32_logsecond value to 25.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = SCR32

DB20000I  The UPDATE DATABASE CONFIGURATION command completed successfully.
Setting warehous_ibm_default_buf_pool value to 50000.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = WAREHOUS

DB20000I  The SQL command completed successfully.
Setting warehous_logsecond value to 25.

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.6
 SQL authorization ID   = DB2APM
 Local database alias   = WAREHOUS

DB20000I  The UPDATE DATABASE CONFIGURATION command completed successfully.
Stopping service apmui (PID 48442).
Service apmui is stopped.
Stopping service min (PID 47105).
Service min is stopped.
Stopping service server1 (PID 44961).
Service server1 is stopped.
Stopping service mongodb (PID 44260).
Service mongodb is stopped.
Starting service mongodb
```

```
Service mongodb is started (PID 9000).
Starting service server1
.......................
Service server1 is started (PID 9256).
Starting service min
......
Service min is started (PID 12376).
Starting service apmui
.....................................................
Service apmui is started (PID 16226).
```

Modification de l'adresse IP et du nom d'hôte du serveur

Vous pouvez à tout moment modifier l'adresse IP et le nom d'hôte du serveur Cloud APM. Si vous modifiez l'adresse IP et le nom d'hôte du serveur, vous devez également modifier l'adresse IP et le nom d'hôte utilisés par tous les agents pour se connecter au serveur Cloud APM.

Avant de commencer

Si vous modifiez l'adresse IP et le nom d'hôte du serveur Cloud APM et que vous prévoyez d'installer de nouveaux agents, créez des packages de configuration pour les images d'agent (voir l'étape 2 dans «Configuration des images téléchargées», à la page 162). Sinon, les agents ne se connecteront pas au serveur ou ne s'afficheront pas dans la console Cloud APM.

Procédure

Procédez comme suit en tant que superutilisateur sur le serveur Cloud APM :

1. Arrêtez tous les composants serveur en entrant la commande suivante dans le répertoire `/usr/bin` :

   ```
   apm stop_all
   ```

2. Démarrez les composants `kafka` et `server1` en entrant les commandes suivantes :

   ```
   apm start kafka
   apm start server1
   ```

3. Modifiez l'adresse IP et le nom d'hôte du serveur utilisé pour démarrer la console Cloud APM. Il s'agit de l'adresse que les utilisateurs entrent pour démarrer la console depuis leurs navigateurs Web. Basculez vers le répertoire *rép_install*`/ccm` et exécutez la commande suivante :

   ```
   configure_server_address.sh
   ```

   Vous êtes invité à entrer les valeurs suivantes :

   - Nom de domaine complet, par exemple : `myserver.example.com`.
   - Nom d'hôte abrégé
   - Adresse IP

   Conseil : Le nom de domaine complet et le nom d'hôte abrégé sont résolus à l'aide du DNS. Si votre système n'a pas la bonne résolution DNS, entrez l'adresse IP pour chacune des trois valeurs.

4. Mettez à jour les noms de fichier de l'agent de serveur. Les agents de serveur sont notamment l'agent Synthetic Events, l'agent Transaction Events et éventuellement l'agent Bluemix Integration. Basculez vers le répertoire *rép_install*`/serveragents/bin` et exécutez la commande suivante :

   ```
   update_config_files.sh
   ```

5. Redéfinissez les références au serveur Cloud APM sur le serveur Db2 local sur la nouvelle adresse IP et le nouveau nom d'hôte :

   a. Mettez à jour la variable de registre *DB2SYSTEM* pour le serveur Db2 local afin qu'elle corresponde au nouveau nom d'hôte du serveur Cloud APM :

      ```
      source /home/db2apm/sqllib/db2profile
      db2set -g DB2SYSTEM=nom_hôte
      ```

où *nom_hôte* est le nouveau nom d'hôte du serveur.

b. Sur votre serveur Db2 local, modifiez le nom d'hôte sur le serveur Cloud APM en éditant le fichier `/home/db2apm/sqllib/db2nodes.cfg` et en remplaçant l'ancien nom d'hôte du serveur par le nouveau.

c. Sur votre serveur Db2 local, mettez à jour le fichier de configuration de l'administrateur Db2 en entrant les commandes suivantes :

```
su - db2apm -c 'db2 update admin cfg using DB2SYSTEM nom_hôte'
su - db2apm -c 'db2 update admin cfg using SMTP_SERVER nom_hôte'
```

où *nom_hôte* est le nouveau nom d'hôte du serveur.

6. Vérifiez que les agents serveur ayant été installés à l'aide du serveur Cloud APM sont configurés pour communiquer avec le serveur à l'aide de l'`hôte local`. Ouvrez le fichier *rép_install*`/serveragents/config/global.environment` puis recherchez les propriétés `IRA_ASF_SERVER_URL` et `IRA_API_DATA_BROKER_URL`. Effectuez l'une des étapes suivantes :
   - Si les propriétés contiennent `localhost` dans la chaîne d'URL, aucune modification n'est nécessaire.
   - Si les propriétés contiennent l'adresse IP du serveur Cloud APM, ce qui est certainement le cas si vous avez configuré les agents pour communiquer via HTTPS, modifiez les adresses IP en `localhost`.
7. Redémarrez les composants serveur en entrant la commande suivante dans le répertoire `/usr/bin` :

```
apm restart_all
```

8. Redéfinissez le nom d'hôte du serveur Cloud APM dans le composant Central Configuration Services.
   a. Le cas échéant, connectez-vous à la console Cloud APM. (Voir «Démarrage de la console Cloud APM», à la page 989.)
   b. Cliquez sur **Configuration système** > **Configuration avancée** et **Configuration centrale d'agent**.
   c. Dans la zone **Substitution du nom d'hôte**, entrez la nouvelle adresse IP ou le nom d'hôte complet du serveur Cloud APM.

   Après avoir cliqué sur **Sauvegarder**, le nouveau nom d'hôte est mis à jour dans le composant Central Configuration Services.
9. Sur les systèmes où vos agents sont installés, connectez les agents à la nouvelle adresse IP et au nouveau nom d'hôte du serveur. Voir «Connexion des agents à un autre serveur», à la page 220.
10. Si des packages de rapports pour l'agent Response Time Monitoring et l'agent WebSphere Applications sont installés, vous devez les réinstaller pour les deux agents. Pour plus d'informations, voir «Installation des rapports», à la page 920. Redémarrez le serveur Tivoli Common Reporting, puis effectuez les étapes présentées dans les sous-rubriques sous Redémarrage des serveurs d'applications Jazz for Service Management.

Résultats

L'adresse IP et le nom d'hôte du serveur sont modifiés.

Configuration du protocole de communications pour les agents de serveur

Le protocole HTTP ou HTTPS est utilisé pour communiquer entre le serveur Cloud APM et les agents de serveur. Le serveur Cloud APM autorise les connexions à partir des agents de serveur qui s'authentifient à l'aide d'un certificat valide. Si vous modifiez le protocole de communication utilisé par le serveur pour communiquer avec les agents de surveillance, vous devez modifier le protocole utilisé par les agents de serveur.

Pourquoi et quand exécuter cette tâche

Les agents de serveur sont des composants du serveur Cloud APM. Les agents de serveur fournissent les fonctions suivantes :

- L'agent Transactions Event fournit des services pour le suivi de transaction.
- L'agent Synthetic Events fournit des services pour les transactions synthétiques.
- L'agent Bluemix Integration intègre le serveur Cloud APM à votre environnement IBM Cloud.

Les agents de serveur sont installés et démarrés automatiquement lorsque vous installez l'offre Cloud APM, Advanced. Si vous disposez de l'offre Cloud APM, Base, aucun agent de serveur n'est utilisé et vous n'avez pas besoin de configurer les protocoles de communications pour les agents de serveur.

Les certificats par défaut sont générés au cours de l'installation du serveur Cloud APM. Les agents de serveur pourraient utiliser les certificats par défaut ou des certificats personnalisés ou autosignés pour se connecter au serveur Cloud APM.

Effectuez les étapes suivantes pour configurer le protocole de communication entre les agents de serveur et le serveur Cloud APM :

Procédure

- Pour passer de la communication HTTPS à la communication HTTP entre le serveur Cloud APM et les agents de serveur, procédez comme suit :
  1. Sur le serveur Cloud APM, ouvrez une fenêtre de commande et basculez vers le répertoire *rép_install*/serveragents/bin. Par exemple :

     ```
     cd /opt/ibm/apm/serveragents/bin
     ```

  2. Exécutez les commandes suivantes pour arrêter les agents de serveur.

     ```
     apm stop biagent
     apm stop soagent
     apm stop txagent
     ```

  3. Exécutez la commande suivante pour configurer la communication HTTP entre le serveur Cloud APM et les agents de serveur :

     ```
     ./agent2server.sh -p HTTP
     ```

  4. Redémarrez les agents de serveur en exécutant les commandes suivantes :

     ```
     apm start biagent
     apm start soagent
     apm start txagent
     ```

- Pour utiliser la communication HTTPS et les certificats par défaut entre le serveur Cloud APM et les agents de serveur, procédez comme suit :
  1. Sur le serveur Cloud APM, ouvrez une fenêtre de commande et basculez vers le répertoire *rép_install*/serveragents/bin. Par exemple :

     ```
     cd /opt/ibm/apm/serveragents/bin
     ```

  2. Exécutez les commandes suivantes pour arrêter les agents de serveur.

     ```
     apm stop biagent
     apm stop soagent
     apm stop txagent
     ```

  3. Exécutez la commande suivante pour configurer la communication HTTPS entre le serveur Cloud APM et les agents de serveur :

     ```
     ./agent2server.sh -p HTTPS
     ```

  4. Redémarrez les agents de serveur en exécutant les commandes suivantes :

     ```
     apm start biagent
     apm start soagent
     apm start txagent
     ```

- Pour utiliser le protocole HTTPS et les certificats autosignés ou les certificats signés par une autorité de certification tierce pour la communication entre le serveur Cloud APM et les agents de serveur, procédez comme suit :
  1. Sur le serveur Cloud APM, ouvrez une fenêtre de commande et arrêtez les agents de serveur en entrant les commandes suivantes :
     ```
     apm stop biagent
     apm stop soagent
     apm stop txagent
     ```
  2. Copiez le contenu du répertoire *rép_install*/ccm/keyfiles/*nom_hôte_serveur*.agent/keyfiles dans le répertoire *rép_install*/serveragents/keyfiles, où *rép_install* correspond au répertoire d'installation du serveur Cloud APM et *nom_hôte_serveur* au nom d'hôte du serveur Cloud APM.
  3. Modifiez le fichier *rép_install*/serveragents/config/global.environment de sorte à spécifier le certificat utilisé par les agents de serveur. Ajoutez ou éditez la variable suivante :
     ```
     KDEBE_KEY_LABEL="Certificat_agent_APM"
     ```

     Important : Si vous avez utilisé un libellé différent de «APM_Agent_Certificate» lorsque vous avez créé les certificats, vous devez spécifier ce libellé à la place de «APM_Agent_Certificate».
  4. Accédez au répertoire *rép_install*/serveragents/bin. Par exemple :
     ```
     cd /opt/ibm/apm/serveragents/bin
     ```
  5. Exécutez la commande suivante pour configurer la communication HTTPS entre le serveur Cloud APM et les agents de serveur :
     ```
     ./agent2server.sh -p HTTPS
     ```
  6. Redémarrez les agents de serveur en exécutant les commandes suivantes :
     ```
     apm start biagent
     apm start soagent
     apm start txagent
     ```

Résultats

Le protocole de communication utilisé pour connecter les agents de serveur au serveur Cloud APM est modifié.

Basculement vers une base de données MongoDB locale

Si votre serveur Cloud APM est connecté à une base de données MongoDB sur un serveur distant, vous pouvez à tout moment basculer sur la base de données MongoDB locale.

Procédure

Effectuez les étapes suivantes en tant que superutilisateur sur le système où vous avez installé le serveur Cloud APM :

1. Accédez au répertoire *rép_install*/mongodb/bin. Par exemple :
   ```
   cd install_dir/mongodb/bin
   ```
2. Supprimez le fichier /mongodb/mongodb-remote.
3. Exécutez la commande **activate-mongodb.sh** pour appliquer la modification.
4. Configurez les communications entre la base de données MongoDB locale et le serveur Cloud APM :
   a. Le cas échéant, connectez-vous à la console Cloud APM. (Voir «Démarrage de la console Cloud APM», à la page 989.)
   b. Cliquez sur **Configuration système** > **Configuration avancée**, puis sur **Mongo Configuration** (Configuration Mongo).
   c. Dans la zone **Nom d'hôte**, entrez localhost.
   d. Cliquez sur **Sauvegarder** pour sauvegarder la configuration.

Lorsque vous avez cliqué sur **Sauvegarder**, les composants de suivi de transaction commencent à communiquer avec la base de données MongoDB locale.

5. Si la base de données MongoDB distante utilisait un mot de passe personnalisé plutôt que le mot de passe `mongoUsrpasswd@08` par défaut, exécutez le script `rép_install/ccm/mongopasswd.sh` pour configurer la base de données MongoDB locale et le serveur Cloud APM pour l'utilisation de votre mot de passe.

Résultats

Le serveur Cloud APM est connecté à la base de données MongoDB locale.

Après le basculement vers la version locale de MongoDB, les *nouveaux* événements de seuil et les *nouvelles* données de suivi de transaction sont transférés entre le serveur Cloud APM et la base de données MongoDB locale.

Les événements ouverts et les données de suivi de transaction qui existent ne sont pas migrés vers MongoDB sur le système local. Pour afficher les événements ouverts existants dans la console Cloud APM, utilisez la commande **touch** de Linux afin de modifier la date et l'heure de tous les fichiers `private_situation.xml` des sous-répertoires sous le répertoire *`rép_install`* `/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source`.

Tâches associées:

«Installation d'une base de données MongoDB distante», à la page 152
MongoDB est une base de données open source NoSQL installée avec le serveur Cloud APM. MongoDB stocke les données de la fonction de suivi de transaction fournie avec l'offre, ainsi que les données d'événement de seuil. Vous pouvez installer et configurer MongoDB sur un système distant à partir du serveur.

Conservation des transactions de middleware

Si vous souhaitez afficher les détails d'instance des transactions de middleware au delà des quatre dernières heures dans le tableau de bord Analyse d'instance des agents de middleware, vous devez modifier la période de conservation dans la base de données MongDB.

Pourquoi et quand exécuter cette tâche

Vous pouvez conserver les données de transaction de middleware pour les agents autorisant le suivi des transactions, tels qu'Agent WebSphere MQ ou agent DataPower dans la base de données MongoDB pendant plus de quatre heures. Pour la liste complète des agents autorisant le suivi des transactions, voir «Suivi des transactions», à la page 61 ou «Fonctions», à la page 40.

Pour modifier la période de conservation des données de suivi des transactions de middleware, effectuez les étapes ci-après.

Procédure

1. Utilisez la feuille de calcul Database Load Projections pour vérifier que votre espace disque est suffisant pour sauvegarder davantage de données dans la base de données MongoDB. La configuration de stockage requise pour la base de données MongoDB est entrée dans les onglets MongoDB et DatamartDB de la feuille de calcul.
2. Editez le fichier `install_dir/mongodb/scripts/cron/mongodb.cfg` et remplacez la valeur par défaut de 18 000 secondes des propriétés IIDOCRETSECS et MIDDOCRETSECS par la valeur de 82 800 secondes pour conserver les données des collections de middleware MongoDB des 23 dernières heures. La 24e collection sera utilisée pour sauvegarder les données à partir de l'heure actuelle. Vous ne devez pas augmenter les valeurs des autres propriétés de conservation dans le fichier `mongodb.cfg` car elles n'affecteront pas les données affichées dans le tableau de bord des transactions.

Sauvegarde et restauration de composants

La sauvegarde et la restauration des fichiers de données et des bases de données est une opération cruciale pour tout système métier, en particulier s'il s'agit de données et d'applications exécutées dans un environnement de production. Créez et suivez un plan de sauvegarde et de récupération des données de tous les composants de votre infrastructure Cloud APM.

Pour planifier la reprise après incident, envisagez de sauvegarder régulièrement les données sur votre serveur Cloud APM et d'enregistrer le fichier de sauvegarde sur une unité montée ou de le copier sur un autre serveur. Si votre serveur Cloud APM utilise un serveur Db2 distant, vous devez également effectuer des sauvegardes sur ce dernier. Pour plus d'informations, voir «Sauvegarde des composants», à la page 1104.

Le serveur Cloud APM stocke les données de configuration dans des fichiers locaux mais aussi dans des bases de données Derby internes locales. Les bases de données du serveur Cloud APM Db2 contiennent les données suivantes :

- Les bases de données DATAMART et de préextraction (WAREHOUS) contiennent les données de mesure de suivi des transactions et de surveillance des ressources. Si vous avez modifié les valeurs de conservation des données d'historique, la base de données WAREHOUS contient également les données de configuration.
- La base de données SCR32 contient le groupe de ressources et les définitions d'application.

Les données de configuration locales du serveur Cloud APM doivent toujours être synchronisées avec les données de configuration des bases de données Db2 lorsque le serveur Db2 est distant.

Si vous disposez d'un fichier de sauvegarde très récent pour le serveur Cloud APM et que vous devez récupérer les données de configuration locales sur ce serveur uniquement, vous pouvez suivre une procédure de reprise qui restaure les données sur ce seul serveur et non sur un serveur Db2 distant. Sinon, suivez l'un des scénarios de reprise suivants qui restaurent les données de configuration sur le serveur Cloud APM et le serveur Db2 distant.

Le serveur Cloud APM sur lequel s'effectue la sauvegarde est appelé serveur source. Le serveur Cloud APM sur lequel s'effectue la reprise est appelé serveur cible. En cas de défaillance matérielle du serveur source, le serveur cible peut être installé sur un autre système. Ils peuvent aussi être installés sur le même système. Le serveur cible doit être au même niveau d'édition et de correctif temporaire que le serveur Cloud APM source, et utiliser le même type de base de données (locale ou distante) et la même version de base de données.

Si un serveur Db2 distant est configuré pour le serveur source, le serveur cible peut utiliser un serveur Db2, une instance et des bases de données identiques ou non en fonction des besoins de reprise des bases de données Cloud APM Db2.

La reprise est une action perturbatrice. Les composants du serveur Cloud APM sont arrêtés et démarrés à plusieurs reprises au cours de cette opération. Choisissez l'une des méthodes de reprise suivantes pour restaurer les données de configuration à partir d'un fichier de sauvegarde.

Tableau 224. Scénarios, approches et procédures à suivre pour la reprise.

Remarque : Vous devez installer le correctif temporaire 6 ou suivant d'IBM Cloud Application Performance Management Private, V8.1.4.0 pour disposer des correctifs nécessaires à l'exécution d'une reprise après incident si le serveur Cloud APM est opérationnel et à l'exécution du script `restore.sh` sur le serveur Db2 distant lorsque vous êtes connecté en tant qu'utilisateur de l'instance Db2.

Remarque : Un serveur Cloud APM est opérationnel si vous pouvez utiliser la console Cloud APM pour ouvrir une session et afficher les données de surveillance, les vues personnalisées, les événements, les seuils, les groupes de ressources, les scripts synthétiques et les règles de contrôle d'accès basées sur les rôles.

Scénario de reprise	Approche de reprise	Procédures de reprise à effectuer
Le serveur Cloud APM est configuré pour utiliser un serveur Db2 local et le serveur Cloud APM est opérationnel.	Si le serveur Cloud APM est opérationnel et que vous souhaitez restaurer une version antérieure des données de configuration, exécutez le script `restore.sh` sur le serveur Cloud APM. Le script de restauration restaure les données de configuration du serveur Cloud APM et les données des bases de données Db2 locales.	Voir Restauration des composants pour la reprise après incident.
Le serveur Cloud APM est configuré pour utiliser un serveur Db2 local et le serveur Cloud APM n'est pas opérationnel.	Si le serveur Cloud APM n'est pas opérationnel et requiert une reprise complète, vous devez le réinstaller et exécuter ensuite le script de restauration pour restaurer les données de configuration et les bases de données Db2. En l'absence de défaillance matérielle, vous pouvez réinstaller le serveur Cloud APM sur le serveur source ou l'installer sur un autre système. Si vous devez installer le serveur Cloud APM sur un autre système, configurez le serveur Cloud APM cible pour utiliser les mêmes nom d'hôte et adresse IP que le serveur Cloud APM source. Sinon, Cloud APM ne sera pas entièrement fonctionnel après la reprise après incident tant que vous n'aurez pas reconfiguré vos systèmes gérés pour qu'ils pointent vers un serveur Cloud APM différent et demandé aux utilisateurs de la console Cloud APM de se connecter avec une adresse URL différente.	Suivez ces procédures dans l'ordre suivant : 1. Voir «Installation du serveur Cloud APM pour la reprise après incident», à la page 1113. 2. Voir Restauration des composants pour la reprise après incident. 3. Si le serveur cible n'est pas le même système que le serveur source et que vous ne pouvez pas modifier le nom d'hôte et l'adresse IP du serveur cible, reportez-vous à «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.
Le serveur Cloud APM est configuré pour utiliser un serveur Db2 distant et le serveur Cloud APM est opérationnel.	Si ce dernier est opérationnel et que vous souhaitez restaurer une version antérieure des données de configuration, exécutez le script `restore.sh` sur le serveur Db2 distant si une reprise des bases de données est nécessaire, puis le script de restauration sur le serveur Cloud APM.	Voir Restauration des composants pour la reprise après incident.

Tableau 224. Scénarios, approches et procédures à suivre pour la reprise (suite).

Remarque : Vous devez installer le correctif temporaire 6 ou suivant d'IBM Cloud Application Performance Management Private, V8.1.4.0 pour disposer des correctifs nécessaires à l'exécution d'une reprise après incident si le serveur Cloud APM est opérationnel et à l'exécution du script `restore.sh` sur le serveur Db2 distant lorsque vous êtes connecté en tant qu'utilisateur de l'instance Db2.

Remarque : Un serveur Cloud APM est opérationnel si vous pouvez utiliser la console Cloud APM pour ouvrir une session et afficher les données de surveillance, les vues personnalisées, les événements, les seuils, les groupes de ressources, les scripts synthétiques et les règles de contrôle d'accès basées sur les rôles.

Scénario de reprise	Approche de reprise	Procédures de reprise à effectuer
Le serveur Cloud APM est configuré pour utiliser un serveur Db2 distant, le serveur Cloud APM n'est pas opérationnel et une reprise des bases de données Db2 distantes n'est pas nécessaire.	Si le serveur Cloud APM n'est pas opérationnel mais que les bases de données Db2 sur le serveur Db2 distant sont en bon état, vous devez réinstaller le serveur Cloud APM et exécuter le script de restauration sur ce dernier uniquement. Le schéma de base de données étant réinitialisé au cours de l'installation du serveur Cloud APM, vous devez installer ce dernier pour utiliser un serveur Db2 local. Une fois l'installation terminée, reconfigurez-le pour utiliser le serveur Db2 distant existant. Exécutez enfin le script de restauration sur le serveur Cloud APM. En l'absence de défaillance matérielle, vous pouvez réinstaller le serveur Cloud APM sur le serveur source ou l'installer sur un autre système. Si vous devez installer le serveur Cloud APM sur un autre système, configurez le serveur Cloud APM cible pour utiliser les mêmes nom d'hôte et adresse IP que le serveur Cloud APM source. Sinon, Cloud APM ne sera pas entièrement fonctionnel après la reprise après incident tant que vous n'aurez pas reconfiguré vos systèmes gérés pour qu'ils pointent vers un serveur différent et demandé aux utilisateurs de la console Cloud APM de se connecter avec une adresse URL différente.	Suivez ces procédures dans l'ordre suivant : 1. Voir «Installation du serveur Cloud APM pour la reprise après incident», à la page 1113 2. Voir «Catalogage des bases de données Db2 après modification du serveur Db2», à la page 1085 3. Voir «Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2», à la page 1087 4. Voir Restauration des composants pour la reprise après incident. 5. Si le serveur cible n'est pas le même que le serveur source et que vous ne pouvez pas modifier le nom d'hôte et l'adresse IP du serveur cible, reportez-vous à «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.

Tableau 224. Scénarios, approches et procédures à suivre pour la reprise (suite).

Remarque : Vous devez installer le correctif temporaire 6 ou suivant d'IBM Cloud Application Performance Management Private, V8.1.4.0 pour disposer des correctifs nécessaires à l'exécution d'une reprise après incident si le serveur Cloud APM est opérationnel et à l'exécution du script `restore.sh` sur le serveur Db2 distant lorsque vous êtes connecté en tant qu'utilisateur de l'instance Db2.

Remarque : Un serveur Cloud APM est opérationnel si vous pouvez utiliser la console Cloud APM pour ouvrir une session et afficher les données de surveillance, les vues personnalisées, les événements, les seuils, les groupes de ressources, les scripts synthétiques et les règles de contrôle d'accès basées sur les rôles.

Scénario de reprise	Approche de reprise	Procédures de reprise à effectuer
Le serveur Cloud APM est configuré pour utiliser un serveur Db2 distant, le serveur Cloud APM n'est pas opérationnel et une reprise des bases de données Db2 distantes est nécessaire.	Dans le cadre de ce scénario, vous pouvez utiliser ou non les mêmes serveur Db2 distant et bases de données qui sont configurés pour le serveur source. Si vous utilisez ces mêmes éléments, supprimez les bases de données Db2 distantes existantes. En l'absence de défaillance matérielle, vous pouvez réinstaller le serveur Cloud APM sur le serveur source ou l'installer sur un autre système. Avant d'installer le serveur Cloud APM, vous devez créer les bases de données sur le serveur Db2 distant. Une fois l'installation terminée, exécutez le script `restore.sh` sur le serveur Db2 distant et sur le serveur Cloud APM. Si vous devez installer le serveur Cloud APM sur un autre système, configurez le serveur Cloud APM cible pour utiliser les mêmes nom d'hôte et adresse IP que le serveur Cloud APM source. Sinon, Cloud APM ne sera pas entièrement fonctionnel après la reprise après incident tant que vous n'aurez pas reconfiguré vos systèmes gérés pour qu'ils pointent vers un serveur différent et demandé aux utilisateurs de la console Cloud APM de se connecter avec une adresse URL différente.	Suivez ces procédures dans l'ordre suivant : 1. Voir la rubrique «Installation du serveur Cloud APM pour la reprise après incident», à la page 1113 qui vous renvoie également à «Connexion à un serveur Db2 distant», à la page 129. 2. Voir Restauration des composants pour la reprise après incident. 3. Si le serveur cible n'est pas le même que le serveur source et que vous ne pouvez pas modifier le nom d'hôte et l'adresse IP du serveur cible, reportez-vous à «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096.

Une solution à haute disponibilité qui utilise la sauvegarde et la restauration est également disponible pour votre serveur Cloud APM. Pour plus d'informations, voir le document APM High Availability Installation and Upgrade.

Pour de plus amples informations sur la sauvegarde et la restauration lors de la mise à niveau de votre serveur Cloud APM, voir «Mise à niveau de votre serveur», à la page 941.

Sauvegarde des composants

Les données de configuration et de mesure du serveur Cloud APM sont sauvegardées à l'aide du script `backup.sh`.

Avant de commencer

Avant de sauvegarder le serveur Cloud APM ou les bases de données Db2 sur un serveur Db2 distant, veillez à créer un emplacement sur votre système de fichiers, comme une unité NFS montée, pour stocker la sortie de la commande de sauvegarde. Le fichier de sauvegarde contenant les données de la base de données Db2 peut être volumineux.

Lorsque vous sauvegardez les bases de données Db2 du serveur Cloud APM, vous pouvez effectuer une sauvegarde hors ligne ou une sauvegarde en ligne. Par défaut, Db2 est configuré pour les sauvegardes hors ligne. Pour effectuer une sauvegarde hors ligne des bases de données, le script `backup.sh` de Cloud APM met en veille par défaut l'activité au niveau des bases de données. Toutefois, les sauvegardes de base de données risquent d'échouer s'il existe des connexions à la base de données lors de l'exécution de la sauvegarde hors ligne. Si un incident se produit, répétez la sauvegarde. Si l'incident persiste, le script `backup.sh` fournit l'option `-q inst` qui permet de mettre en veille toutes les activités de la base de données au niveau de l'instance de base de données. Une mise en veille au niveau de l'instance peut être plus efficace pour arrêter toutes les connexions de base de données mais elle empêche tous les utilisateurs de se connecter à l'instance de base de données Db2 et peut empêcher les connexions à d'autres bases de données utilisant l'instance de base de données Db2. Pour plus d'informations sur la commande Db2 **`QUIESCE`**, reportez-vous à la rubrique décrivant la commande QUIESCE.

Vous pouvez également activer la sauvegarde en ligne des bases de données Db2, qui s'exécute en arrière-plan. Au cours de la sauvegarde en ligne, les applications peuvent continuer à accéder à la base de données, ce qui évite les temps d'indisponibilité. Il est recommandé d'effectuer des sauvegardes de bases de données en ligne pour des environnements de production.

Si vous souhaitez effectuer une sauvegarde de base de données en ligne, activez les sauvegardes en ligne en suivant la procédure de la rubrique «Activation de la sauvegarde en ligne des bases de données Db2», à la page 1107. Une fois que vous avez activé les sauvegardes en ligne, le script `backup.sh` du serveur Cloud APM effectue par défaut une sauvegarde de base de données en ligne.

Pourquoi et quand exécuter cette tâche

Effectuez des sauvegardes régulières sur le serveur Cloud APM et le serveur Db2 s'il se trouve sur un système distant. Sauvegardez le fichier de sauvegarde sur un autre serveur ou sur une unité montée afin de pouvoir effectuer une reprise si le serveur Cloud APM est endommagé et qu'il doit être restauré ultérieurement.

Si le serveur Cloud APM utilise un serveur Db2 local, exécutez le script `backup.sh` sur le serveur Cloud APM pour sauvegarder les données de configuration locale et les bases de données Db2. Si le serveur Cloud APM est connecté à un serveur Db2 distant, exécutez le script `backup.sh` sur le serveur Cloud APM pour sauvegarder les données de configuration locales et exécutez également le script `backup.sh` sur le serveur Db2 pour sauvegarder les bases de données Db2.

Procédure

Sauvegardez les données de configuration du serveur Cloud APM et les bases de données Db2 en effectuant les opérations suivantes :

1. En tant que superutilisateur (root), exécutez le script *rép_install*`/ccm/backup.sh` sur le serveur Cloud APM pour générer le fichier de sauvegarde tar. Indiquez les options suivantes :

   ```
   backup.sh -f fichier_sauvegarde -u nom_utilisateur_apmadmin -p mot_de_passe_apmadmin
   -j nom_bdd_entrepôt -k nom_bdd_scr -l nom_bdd_magasin
   -q inst -t rép_tmp
   ```

   Où :

   - `-f` *fichier_sauvegarde* est le nom et le chemin du fichier de sauvegarde TAR. Par défaut, le script crée un fichier de sauvegarde TAR dans le répertoire *rép_install*`/backups`.

- `-u` *nom_utilisateur_apmadmin* est l'ID administrateur. Si vous utilisez le registre de base pour authentifier des utilisateurs de la console Cloud APM, indiquez `apmadmin`. Si vous utilisez LDAP pour authentifier des utilisateurs de la console Cloud APM, indiquez l'utilisateur LDAP configuré en tant que valeur `systemUser` dans le fichier *rép_install*`/wlp/usr/servers/apmui/server-oauth2-tai.xml`. Lorsque vous indiquez le nom d'utilisateur LDAP, indiquez-le dans même format que celui utilisé lors de la connexion à la console Cloud APM. Le nom par défaut est `apmadmin`.
- `-p` *mot_de_passe_apmadmin* est le mot de passe de l'utilisateur indiqué par l'option `-u`. Le mot de passe par défaut est `apmpass`.

  Remarque : Si vous indiquez un mot de passe personnalisé qui inclut des caractères non alphanumériques, vous devez le placer entre apostrophes. Par exemple, `-p 'Z!@12ws*'`
- `-j` *nom_bdd_entrepôt* est le nom de la base de données de l'entrepôt. Le nom par défaut est WAREHOUS.
- `-k` *nom_bdd_scr* est le nom de la base de données SCR. Le nom par défaut est SCR32.
- `-l` *nom_bdd_magasin* est le nom de la base de données du magasin. Le nom par défaut est DATAMART.
- `-q inst` Entrez l'option `-q inst` comme indiqué dans la commande précédente. Ne remplacez pas `inst` par l'instance Db2. Si le serveur Db2 est un serveur local et que vous effectuez une sauvegarde de base de données hors ligne, utilisez cette option pour effectuer la mise au veille au niveau de l'instance Db2 au lieu de celui de la base de données. Par défaut, l'activité est mise en veille au niveau de la base de données mais les sauvegardes de base de données risquent d'échouer si des applications accèdent à la base de données lors de la sauvegarde. Vous devrez donc peut-être indiquer cette option pour mettre en veille toutes les activités de base de données.

  Remarque : Cette option empêche tous les utilisateurs de se connecter à l'instance de base de données Db2 et vous pouvez empêcher les connexions à d'autres bases de données utilisant l'instance de base de données Db2. Pour plus d'informations sur la commande Db2 **`QUIESCE`**, reportez-vous à la rubrique décrivant la commande QUIESCE.
- `-t` *rép_tmp* est le répertoire que vous utilisez pour les fichiers temporaires. Le répertoire par défaut est `/tmp`.

2. Si le serveur Cloud APM est configuré pour utiliser un serveur Db2 distant, procédez comme suit :
   a. Copiez les scripts *rép_install*`/ccm/backup.sh` et `restore.sh` du système où le serveur Cloud APM est installé vers le système où Db2 est installé si le fichier n'a pas été déjà copié. Vérifiez que les scripts disposent de droits permettant à l'utilisateur de l'instance de base de données Db2 de les exécuter. Si vous avez installé récemment un correctif temporaire du serveur Cloud APM, copiez les scripts `backup.sh` et `restore.sh` les plus récents sur le serveur Db2.
   b. Connectez-vous en tant qu'utilisateur de l'instance Db2 sur le système où Db2 est installé.
   c. Exécutez le script `backup.sh` avec les options suivantes pour sauvegarder les bases de données Db2 de Cloud APM.

      ```
      backup.sh -f fichier_sauvegarde -j nom_bdd_entrepôt
       -k nom_bdd_scr -l nom_bdd_magasin -q inst -z nom_instance_Db2_personnalisé -t rép_tmp
      ```

      où :
      - `-f` *fichier_sauvegarde* est le nom et le chemin du fichier de sauvegarde TAR. Par défaut, le script crée un fichier de sauvegarde TAR dans le répertoire *rép_install*`/backups`.
      - `-j` *nom_bdd_entrepôt* est le nom de la base de données de l'entrepôt. Le nom par défaut est WAREHOUS.
      - `-k` *nom_bdd_scr* est le nom de la base de données SCR. Le nom par défaut est SCR32.
      - `-l` *nom_bdd_magasin* est le nom de la base de données du magasin. Le nom par défaut est DATAMART.
      - `-q inst` Entrez l'option `-q inst` comme indiqué dans la commande précédente. Ne remplacez pas `inst` par l'instance Db2. Si vous effectuez une sauvegarde de base de données hors ligne,

utilisez cette option pour mettre en veille les activités de la base de données au niveau de l'instance Db2 au lieu de celui de la base de données. Par défaut, l'activité est mise en veille au niveau de la base de données mais les sauvegardes de la base de données risquent d'échouer si des applications accèdent à la base de données lors de la sauvegarde. Vous devrez donc peut-être indiquer cette option pour mettre en veille toutes les activités de base de données.

Remarque : Cette option empêche tous les utilisateurs de se connecter à l'instance de base de données Db2 et vous pouvez empêcher les connexions à d'autres bases de données utilisant l'instance de base de données Db2. Pour plus d'informations sur la commande Db2 **QUIESCE**, reportez-vous à la rubrique décrivant la commande QUIESCE.

- `-z` *nom_instance_Db2_personnalisé* est l'ID utilisateur de l'instance Db2. L'ID utilisateur par défaut est `db2apm`.
- `-t` *rép_tmp* est le répertoire que vous utilisez pour les fichiers temporaires. Le répertoire par défaut est `/tmp`.

Résultats

La sauvegarde du serveur Cloud APM est complète et les données sont stockées dans un fichier TAR qui permet d'effectuer la reprise du serveur Cloud APM et de ses bases de données Db2.

Que faire ensuite

Lorsque le serveur Cloud APM requiert une procédure de reprise, restaurez les données sauvegardées en suivant les étapes de la rubrique «Restauration des composants pour la reprise après incident», à la page 1109.

Activation de la sauvegarde en ligne des bases de données Db2 :

Par défaut, les bases de données Cloud APM Db2 sont configurées pour une sauvegarde hors ligne, ce qui signifie que leur activité doit être arrêtée au préalable. Vous pouvez activer une sauvegarde en ligne en arrière-plan des bases de données Db2. Au cours de la sauvegarde en ligne, les applications peuvent continuer à accéder à la base de données, ce qui évite les temps d'indisponibilité.

Pourquoi et quand exécuter cette tâche

Plusieurs options de sauvegarde sont disponibles pour les bases de données Cloud APM Db2. Aussi, selon les environnements, la solution incluse dans cette tâche peut nécessiter des modifications.

Pour activer la sauvegarde en ligne, modifiez la configuration de base de données. Cet exemple indique une configuration pour la sauvegarde intégrale. La sauvegarde intégrale nécessite un espace disque substantiel et prend plus de temps, car la base de données entière est sauvegardée à chaque fois. Db2 permet la sauvegarde incrémentielle qui a plusieurs options.

- Pour plus d'informations sur la configuration de la sauvegarde incrémentielle, voir Incremental backup and recovery et Restoring from incremental backup images.
- Pour obtenir la description des paramètres de configuration Db2 utilisés dans cette tâche, voir Paramètres de configuration de base de données Db2.
- Pour accéder à une autre documentation Db2, voir la Collection de rubriques IBM Db2 10.5 for Linux, Unix and Windows dans l'IBM Knowledge Center.

Vous pouvez utiliser les paramètres de configuration Db2 suivants pour la configuration de la sauvegarde en ligne. Tous ces paramètres sont facultatifs, à l'exception du paramètre **LOGARCHMETH1** qui est obligatoire.

LOGARCHMETH1
Ce paramètre obligatoire indique le type de support. Redéfinissez l'unité indiquée sur cette propriété sur un répertoire approprié.

AUTO_DEL_REC_OBJ
Ce paramètre facultatif indique si des fichiers de consignation de journal de base de données, les images de sauvegarde et les images de copie de chargement doivent être supprimés quand leur entrée associée de fichier historique de récupération est élaguée.

REC_HIS_RETENTN
Ce paramètre facultatif indique la durée de conservation (en jours) des informations historiques sur les sauvegardes.

NUM_DB_BACKUPS
Ce paramètre facultatif indique le nombre de sauvegardes complètes à conserver pour une base de données.

LOGARCHCOMPR1
Ce paramètre facultatif indique si les fichiers journaux écrits dans la destination principale d'archivage des journaux sont compressés.

Conseil : La procédure suivante permet d'archiver les fichiers journaux sur disque de manière permanente. Vous pouvez élaguer les fichiers journaux et les fichiers historiques à l'aide de commandes Db2. Pour plus d'informations, voir PRUNE HISTORY/LOGFILE.

Procédure

1. Pour configurer la base de données SCR32 pour la sauvegarde en ligne, exécutez la commande suivante en tant qu'utilisateur db2apm. Le chemin de répertoire dans la commande suivante est fourni à titre d'exemple uniquement. L'administrateur Db2 peut sélectionner le répertoire qui doit contenir les journaux de la base de données.

   ```
   mkdir -p /rép_db2/logs/SCR32/archive
   ```

   où *rép_db2* est le répertoire qui contient tous les fichiers journaux de la base de données.

   Démarrez l'interpréteur de commandes Db2 (commande **db2**) et exécutez les commandes Db2 suivantes :

   ```
   CONNECT TO SCR32;
   UPDATE DB CFG FOR SCR32 USING LOGARCHMETH1 'DISK:/<rép_db2>/logs/SCR32/archive';
   UPDATE DB CFG FOR SCR32 USING AUTO_DEL_REC_OBJ ON;
   UPDATE DB CFG FOR SCR32 USING REC_HIS_RETENTN 10;
   UPDATE DB CFG FOR SCR32 USING NUM_DB_BACKUPS 10;
   UPDATE DB CFG FOR SCR32 USING LOGARCHCOMPR1 OFF;
   DISCONNECT CURRENT;
   ```

2. Pour configurer la base de données WAREHOUS pour la sauvegarde en ligne, exécutez la commande Db2 suivante en tant qu'utilisateur db2apm. Le chemin de répertoire dans la commande suivante est fourni à titre d'exemple uniquement. L'administrateur Db2 peut sélectionner le répertoire qui doit contenir les journaux de la base de données.

   ```
   mkdir -p /rép_db2/logs/WAREHOUS/archive
   ```

   Démarrez l'interpréteur de commandes Db2 (commande **db2**) et exécutez les commandes suivantes :

   ```
   CONNECT TO WAREHOUS;
   UPDATE DB CFG FOR WAREHOUS USING LOGARCHMETH1 'DISK:/<rép_db2>/logs/WAREHOUS/archive';
   UPDATE DB CFG FOR WAREHOUS USING AUTO_DEL_REC_OBJ ON;
   UPDATE DB CFG FOR WAREHOUS USING REC_HIS_RETENTN 10;
   UPDATE DB CFG FOR WAREHOUS USING NUM_DB_BACKUPS 10;
   UPDATE DB CFG FOR WAREHOUS USING LOGARCHCOMPR1 OFF;
   DISCONNECT CURRENT;
   ```

3. Pour configurer la base de données DATAMART pour la sauvegarde en ligne, exécutez la commande Db2 suivante en tant qu'utilisateur db2apm : Le chemin de répertoire dans la commande suivante est fourni à titre d'exemple uniquement. L'administrateur Db2 peut sélectionner le répertoire qui doit contenir les journaux de la base de données.

   ```
   mkdir -p /rép_db2/logs/DATAMART/archive
   ```

Démarrez l'interpréteur de commandes Db2 (commande **db2**) et exécutez les commandes suivantes :

```
CONNECT TO DATAMART;
UPDATE DB CFG FOR DATAMART USING LOGARCHMETH1 'DISK:/<rép_db2>/logs/DATAMART/archive';
UPDATE DB CFG FOR DATAMART USING AUTO_DEL_REC_OBJ ON;
UPDATE DB CFG FOR DATAMART USING REC_HIS_RETENTN 10;
UPDATE DB CFG FOR DATAMART USING NUM_DB_BACKUPS 10;
UPDATE DB CFG FOR DATAMART USING LOGARCHCOMPR1 OFF;
DISCONNECT CURRENT;
```

4. Exécutez une sauvegarde initiale hors ligne de base de données, une fois que vous avez configuré la base de données pour une sauvegarde en ligne. Arrêtez les processus qui utilisent les bases de données. Pour exécuter la sauvegarde initiale hors connexion, exécutez les commandes suivantes :
   a. En tant que superutilisateur, exécutez les commandes suivantes :

      ```
      apm stop_all
      apm start db2
      ```

   b. En tant qu'utilisateur db2apm, exécutez les commandes suivantes :

      ```
      db2 backup db SCR32 to /dev/null
      db2 backup db WAREHOUS to /dev/null
      db2 backup db DATAMART to /dev/null
      ```

   c. En tant que superutilisateur, exécutez la commande suivante :

      ```
      apm start_all
      ```

Résultats

Les bases de données sont désormais prêtes pour la sauvegarde en ligne. Au cours de l'exécution du script `backup.sh` Cloud APM, une sauvegarde de base de données en ligne est effectuée.

Restauration des composants pour la reprise après incident

Si la reprise après incident est requise pour les données de configuration de votre serveur Cloud APM, exécutez le script `restore.sh` pour restaurer les composants du serveur et leurs bases de données avec les données de configuration contenues dans un fichier de sauvegarde récent.

Avant de commencer

Pour effectuer la reprise, vous devez disposer d'un fichier de sauvegarde récent. Si votre serveur Cloud APM utilise un serveur Db2 distant, vous devez disposer d'un fichier de sauvegarde pour votre serveur Cloud APM et, en option, d'un fichier de sauvegarde pour votre serveur Db2 distant. Vous devez effectuer des sauvegardes régulières pour que des fichiers de sauvegarde soient disponibles si une reprise est nécessaire. Pour plus d'informations sur la manière de créer des fichiers de sauvegarde, voir «Sauvegarde des composants», à la page 1104.

Dans cette rubrique, le serveur source indique le serveur Cloud APM sur lequel le fichier de sauvegarde a été créé et le serveur cible indique le serveur Cloud APM sur lequel la reprise est effectuée. Les serveurs source et cible peuvent être le même système ou des systèmes différents.

Pour connaître les scénarios de reprise et choisir l'approche à utiliser, voir «Sauvegarde et restauration de composants», à la page 1101. Si vous avez choisi une approche consistant à réinstaller le serveur Cloud APM sur le même système ou à l'installer sur un autre système, vous devez terminer son installation avant d'exécuter le script `restore.sh`. Pour obtenir des instructions, voir «Installation du serveur Cloud APM pour la reprise après incident», à la page 1113.

Si votre serveur Cloud APM utilise un serveur Db2 distant et que vous devez effectuer une reprise pour les bases de données, exécutez le script `restore.sh` sur le serveur Db2 distant, puis sur le serveur Cloud APM.

La reprise est une action perturbatrice. Les composants du serveur Cloud APM sont arrêtés et démarrés à plusieurs reprises au cours de cette opération.

Procédure

Suivez la procédure ci-dessous. Pour les étapes à suivre sur le serveur Cloud APM, vous devez être l'utilisateur root.

1. Sur le serveur Cloud APM cible, arrêtez tous les composants de serveur en lançant la commande ci-dessous.

   ```
   apm stop_all
   ```

2. Si le serveur Cloud APM cible est installé sur autre système que le serveur Cloud APM source, procédez comme suit :
   a. Si le serveur Cloud APM source est encore opérationnel, arrêtez tous les composants du serveur en lançant la commande suivante sur ce dernier :

      ```
      apm stop all
      ```

      Arrêtez le système.
   b. Configurez le serveur Cloud APM cible pour utiliser les mêmes nom d'hôte et adresse IP que le serveur Cloud APM source. Si vous ne pouvez pas modifier le nom d'hôte et l'adresse IP du serveur cible, vous devez reconfigurer tous vos agents et collecteurs de données pour qu'ils se connectent au nom d'hôte ou à l'adresse IP du serveur Cloud APM cible une fois la restauration terminée. Pour plus de détails, voir le premier paragraphe de la section Etape suivante.
3. Si votre serveur Cloud APM cible est configuré pour utiliser un serveur Db2 distant et que vous devez effectuer une reprise de vos bases de données Cloud APM Db2, suivez la procédure ci-dessous sur le serveur Db2 distant en tant qu'ID utilisateur de l'instance Db2.
   a. Copiez le fichier de sauvegarde pour vos bases de données Cloud APM Db2 sur le serveur Db2 ou vérifiez qu'il est possible d'y accéder à partir d'une unité montée. L'ID utilisateur de l'instance Db2 doit avoir un accès en lecture au fichier.
   b. Copiez le script *rép_install*/ccm/restore.sh à partir du serveur serveur Cloud APM cible vers le serveur Db2 et vérifiez que l'utilisateur de l'instance Db2 dispose des droits nécessaires pour l'exécuter.
   c. Exécutez le script restore.sh avec les options suivantes :

      ```
      restore.sh -f fichier_sauvegarde -j nom_bd_warehouse
       -k nom_bd_scr -l nom_bd_datamart -q inst
       -z nom_instance_Db2_personnalisée -1 chemin_journal_bd_warehouse -2 chemin_journal_bd_scr -3 chemin_journal_bd_data
      ```

      Où :

      - -f *fichier_sauvegarde* est le nom et le chemin d'accès au fichier TAR de sauvegarde. Cette option est obligatoire.
      - -j *nom_bd_warehouse* est le nom de la base de données Warehouse. Le nom par défaut est WAREHOUS.
      - -k *nom_bd_scr* est le nom de la base de données SCR. Le nom par défaut est SCR32.
      - -l *nom_bd_datamart* est le nom de la base de données Datamart. Le nom par défaut est DATAMART.
      - -q inst Entrez -q inst comme indiqué dans la commande précédente. Ne remplacez pas inst par l'instance Db2. Utilisez cette option pour mettre au repos l'activité de la base de données au niveau de l'instance Db2 plutôt qu'au niveau de la base de données. Par défaut, l'activité est mise au repos au niveau de la base de données mais les restaurations de base de données risquent d'échouer si des applications accèdent à cette dernière au cours du processus. Vous pouvez alors être amené à spécifier cette option pour mettre au repos toute l'activité de la base de données.

        Remarque : Cette option empêche tous les utilisateurs de se connecter à l'instance de base de données Db2 et vous pouvez empêcher les connexions à d'autres bases de données utilisant

l'instance de base de données Db2. Pour plus d'informations sur la commande Db2 **QUIESCE**, reportez-vous à la rubrique décrivant la commande QUIESCE.

- `-z` *nom_instance_Db2_personnalisée* est l'ID utilisateur de l'instance Db2. L'ID utilisateur par défaut est `db2apm`.
- `-1` *chemin_journal_bd_warehouse* est le chemin d'accès aux fichiers journaux pour la base de données indiquée à l'aide de l'option `–j` ou la base de données WAREHOUS si cette option n'est pas spécifiée. Le chemin par défaut est celui du fichier journal utilisé lorsque la sauvegarde de la base de données a été effectuée.
- `-2` *chemin_journal_bd_scr* est le chemin d'accès aux fichiers journaux pour la base de données indiquée à l'aide de l'option `–k` ou la base de données SCR32 si cette option n'est pas spécifiée. Le chemin par défaut est celui du fichier journal utilisé lorsque la sauvegarde de la base de données a été effectuée.
- `-3` *chemin_journal_bd_datamart* est le chemin d'accès aux fichiers journaux pour la base de données indiquée à l'aide de l'option `–l` ou la base de données DATAMART si cette option n'est pas spécifiée. Le chemin par défaut est celui du fichier journal utilisé lorsque la sauvegarde de la base de données a été effectuée.

  Remarque : La restauration de la base de données utilise le même chemin de stockage de base de données qui a été utilisé sur le serveur Db2 où le fichier de sauvegarde a été créé.

4. Sur votre serveur Cloud APM cible, procédez comme suit :
   a. Copiez le fichier de sauvegarde depuis votre serveur Cloud APM vers le système où vous effectuez la reprise ou vérifiez qu'il est possible d'y accéder à partir d'une unité montée. L'utilisateur root doit avoir des droits d'accès en lecture au fichier de sauvegarde.
   b. Exécutez le script `restore.sh` avec les options suivantes :

      ```
      restore.sh -f fichier_sauvegarde -u nomutilisateur_apmadmin -p motdepasse_apmadmin
      -j nom_bd_warehouse -k nom_bd_scr -l nom_bd_datamart -q inst
      ```

   Où :

   - `-f` *fichier_sauvegarde* nom et chemin d'accès au fichier TAR de sauvegarde pour le serveur Cloud APM. Cette option est obligatoire.
   - `-u` *nom_utilisateur_apmadmin* est l'ID administrateur. Si vous utilisez le registre de base pour authentifier des utilisateurs de la console Cloud APM, indiquez `apmadmin`. Si vous utilisez LDAP pour authentifier des utilisateurs de la console Cloud APM, indiquez l'utilisateur LDAP configuré en tant que valeur `systemUser` dans le fichier *rép_install*`/wlp/usr/servers/apmui/server-oauth2-tai.xml`. Lorsque vous indiquez le nom d'utilisateur LDAP, indiquez-le dans même format que celui utilisé lors de la connexion à la console Cloud APM. Le nom par défaut est `apmadmin`.
   - `-p` *mot_de_passe_apmadmin* est le mot de passe de l'utilisateur indiqué par l'option `-u`. Le mot de passe par défaut est `apmpass`.

     Remarque : Si vous indiquez un mot de passe personnalisé qui inclut des caractères non alphanumériques, vous devez le placer entre apostrophes. Par exemple, `-p 'Z!@12ws*'`
   - `-j` *nom_bd_warehouse* est le nom de la base de données Warehouse. Le nom par défaut est WAREHOUS.
   - `-k` *nom_bd_scr* est le nom de la base de données SCR. Le nom par défaut est SCR32.
   - `-l` *nom_bd_datamart* est le nom de la base de données Datamart. Le nom par défaut est DATAMART.
   - `-q inst` Entrez `-q inst` comme indiqué dans la commande précédente. Ne remplacez pas `inst` par l'instance Db2. Si votre serveur Db2 est local, utilisez cette option pour mettre au repos l'activité de la base de données au niveau de l'instance Db2 plutôt qu'au niveau de la base de données. Par défaut, l'activité est mise au repos au niveau de la base de données mais les restaurations de base de données risquent d'échouer si des applications accèdent à cette dernière au cours du processus. Vous pouvez alors être amené à spécifier cette option pour mettre au repos toute l'activité de la base de données.

Remarque : Cette option empêche tous les utilisateurs de se connecter à l'instance de base de données Db2 et vous pouvez empêcher les connexions à d'autres bases de données utilisant l'instance de base de données Db2. Pour plus d'informations sur la commande Db2 **QUIESCE**, reportez-vous à la rubrique décrivant la commande QUIESCE.

5. Si vous avez configuré votre serveur Cloud APM cible pour utiliser des bases de données Db2 distantes différentes de celles du serveur Cloud APM source, certains composants serveur Cloud APM cible sont configurés pour utiliser les bases de données du serveur source une fois la restauration terminée. Suivez la procédure décrite dans «Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2», à la page 1087 pour reconfigurer le serveur Cloud APM cible pour utiliser ses bases de données.
6. Si vous avez effectué la restauration à l'aide d'un fichier de sauvegarde de base de données qui a été créé il y a plus de deux jours, il se peut qu'il ne reste plus de partitions actives dans la base de données WAREHOUS une fois la restauration terminée. Aucune donnée de surveillance des ressources n'est alors visible dans les pages de tableau de bord de la console Cloud APM. Pour forcer le service `ksy` à créer immédiatement des partitions (sans attendre qu'il soit 2 heures du matin), suivez la procédure ci-dessous en tant que superutilisateur sur le serveur Cloud APM.
   a. Lancez la commande `apm stop ksy`.
   b. Editez le fichier *rép_install*`/sy/config/sy.ini` et supprimez la mise en commentaire de `KSY_ON_DEMAND=Y` en supprimant la balise # placée au début de la ligne contenant cette variable d'environnement.
   c. Accédez au répertoire *rép_install*`/sy/bin` en lançant la commande suivante :
      ```
      cd rép_install/sy/bin
      ```
   d. Lancez la commande `itmcmd agent start sy`.
   e. Consultez le dernier fichier journal `*sy_java*` dans le répertoire *rép_install*`/sy/logs`. Si le message suivant apparaît à la fin de ce fichier, les partitions ont été créées avec succès. La création de partitions pour plusieurs agents peut prendre du temps.
      ```
      == 4750 t=Thread-5 Summarization and pruning agent successfully ended
      == 2017-12-03 03.03.02.264 +0800 : Trace paused
      ```
   f. Lancez la commande `itmcmd agent stop sy`.
   g. Editez le fichier *rép_install*`/sy/config/sy.ini` et mettez en commentaire la ligne `KSY_ON_DEMAND=Y` en ajoutant la balise # au début de la ligne contenant cette variable d'environnement.
   h. Lancez la commande `apm start ksy`.

Résultats

La reprise du serveur Cloud APM est terminée. Vous pouvez maintenant accéder aux données de vos agents et autres composants depuis votre serveur Cloud APM.

Que faire ensuite

- Si vous n'avez pas pu effectuer l'étape 2.b, suivez les étapes présentées dans «Modification de l'adresse IP et du nom d'hôte du serveur», à la page 1096 pour mettre à jour l'adresse IP et le nom d'hôte qui ont été utilisés par les composants du serveur Cloud APM cible et par vos agents et collecteurs de données. En outre, si une autre URL est requise pour la connexion, informez-en les utilisateurs de la console Cloud APM.
- Au cours du processus de restauration, les fichiers de clés du serveur Cloud APM sont modifiés, ce qui n'affecte pas les agents et collecteurs de données existants. Toutefois, les fichiers de clés dans les images d'agent et de collecteur de données ne sont pas mis à jour si vous avez installé ou réinstallé le serveur Cloud APM à des fins de reprise. Si vous prévoyez d'installer de nouveaux agents et collecteurs de données avec des communications sécurisées HTTPS entre le serveur Cloud APM et les agents en utilisant les images d'agent ou de collecteur de données qui ont été générées au cours de l'installation du serveur Cloud APM, vous devez reconfigurer celles-ci afin qu'elles récupèrent les fichiers de clés restaurés. Lorsque vous exécutez le script `make_configuration_packages.sh` pour créer

les modules de configuration, veillez à sélectionner le protocole HTTPS. Pour plus d'informations, voir «Configuration des images téléchargées», à la page 162.

- Si votre serveur Cloud APM est configuré pour utiliser le protocole HTTPS pour la communication entre l'agent et le serveur, mettez à jour le protocole de communication et les certificats utilisés par les agents du serveur Cloud APM. Pour plus d'informations, voir «Configuration du protocole de communications pour les agents de serveur», à la page 1097.

Installation du serveur Cloud APM pour la reprise après incident :

Si vous installez un nouveau serveur Cloud APM ou réinstallez un serveur Cloud APM existant pour la reprise après incident, assurez-vous qu'il possède les mêmes version, correctif temporaire, mots de passe et version de base de données que celui sur lequel la sauvegarde a été effectuée.

Pourquoi et quand exécuter cette tâche

Lors d'une reprise après incident, vous restaurez la configuration du serveur Cloud APM à partir d'un fichier de sauvegarde. Dans cette procédure, le serveur source indique le serveur Cloud APM sur lequel le fichier de sauvegarde a été créé et le serveur cible indique le serveur Cloud APM sur lequel la restauration est effectuée. Les serveurs source et cible peuvent être le même système ou des systèmes différents. Pour plus d'informations, voir «Sauvegarde et restauration de composants», à la page 1101.

Lorsque vous installez le serveur Cloud APM sur le serveur cible, vous devez répondre aux exigences suivantes :

- Installez les mêmes version et offre du serveur Cloud APM sur le serveur cible que celles du serveur source. Si un correctif temporaire de serveur Cloud APM est installé sur le serveur source, vous devez installer le même correctif temporaire de serveur Cloud APM sur le serveur cible. Pour télécharger le correctif temporaire requis, accédez à IBM Fix Central.
- Configurez le même type de base de données Db2 (locale ou distante) sur le serveur cible que sur le serveur source. Si vous avez installé un groupe de correctifs Db2 sur le serveur Db2 qui est utilisé par le serveur source Cloud APM, vous devez appliquer le même groupe de correctifs Db2 sur le serveur de base de données que celui utilisé par le serveur cible Cloud APM avant de terminer la restauration afin que les serveurs source et cible utilisent la même version de Db2. Pour plus d'informations sur les groupes de correctifs Db2, consultez Db2 IBM Knowledge Center pour savoir quelle version de Db2 vous exécutez. Par exemple, pour Db2 version 11.1, voir IBM Db2 Version 11.1 Knowledge Center.
- Utilisez sur le serveur cible le même chemin d'installation que sur le serveur source.
- Utilisez sur le serveur cible les mêmes mots de passe pour les ID utilisateur suivants que sur le serveur source :
  - `apmadmin`
  - `smadmin`
  - ID utilisateur MongoDB
  - `itmuser`
  - utilisateur `db2apm` lorsque la base de données du serveur Cloud APM est locale.

Pour plus d'informations, voir «Utilisateurs et mots de passe par défaut», à la page 1075.

Procédure

1. Si le serveur Cloud APM cible est le même que le serveur source, désinstallez-le. Pour obtenir des instructions, voir «Désinstallation du serveur», à la page 148.

   Remarque : Vous devez exécuter les tâches suivantes avant de tenter de réinstaller le serveur Db2 local.

   - Désinstallez le serveur ou le client Db2 s'il est déjà installé.

- Supprimez tous les utilisateurs Cloud APM Db2, tels que `db2apm`, `itmuser`, `dasusr1` et `db2fenc1` du serveur Cloud APM.
- Supprimez tous les groupes d'utilisateurs, tels que `db2iadm1`, `db2fadm1` et `dasadm1` du serveur Cloud APM.
- Supprimez tous les répertoires de base du serveur Cloud APM.

2. Si le serveur Cloud APM source est configuré pour utiliser un serveur Db2 distant, vous disposez de trois options :
   a. Si le serveur Cloud APM cible est installé de manière à être disponible pour une reprise après incident ultérieure et que vous prévoyez de continuer à utiliser le serveur Cloud APM source jusqu'à ce que la reprise soit requise, ou si vous souhaitez que le serveur Cloud APM cible utilise un serveur Db2 distant, une instance ou des bases de données différents, le serveur Cloud APM cible doit être installé et configuré pour utiliser des bases de données Db2 différentes de celles du serveur Cloud APM source. Créez les bases de données en suivant les étapes décrites dans «Connexion à un serveur Db2 distant», à la page 129.
   b. Ou, si vous êtes prêt à effectuer la reprise et que celle-ci est nécessaire pour les bases de données du serveur Cloud APM, le serveur Cloud APM cible peut utiliser les mêmes serveur Db2, utilisateur de l'instance Db2 et noms de base de données que le serveur Cloud APM source. Dans le cadre de ce scénario, procédez comme suit :
      1) Si les composants du serveur Cloud APM source sont encore en cours d'exécution, arrêtez-les tous en lançant la commande **apm stop_all** sur le serveur source.
      2) En collaboration avec votre administrateur, supprimez les trois bases de données du serveur Cloud APM.
      3) Recréez-les en suivant les étapes décrites dans «Connexion à un serveur Db2 distant», à la page 129.
   c. Ou, si vous êtes prêt à effectuer la reprise et souhaitez l'appliquer au serveur Cloud APM uniquement et non au serveur Db2, le serveur Cloud APM cible est configuré pour utiliser le serveur de base de données local au cours de l'installation et reconfiguré pour utiliser les mêmes bases de données que le serveur Cloud APM source une fois l'installation terminée.
3. Procédez à l'installation sur le serveur Cloud APM cible. Commencez par consulter ces rubriques pour déterminer si l'une d'elles est applicable :
   «Définition des communications HTTP ou HTTPS», à la page 128
   «Installation sur un système à l'aide d'un service d'annuaire externe», à la page 138
   «Création d'utilisateurs Db2 avant la connexion à un serveur Db2 local», à la page 140

   Remarque : Si vos utilisateurs Db2 du serveur source possédaient des mots de passe personnalisés, vous devez effectuer les étapes de cette rubrique :
   «Création d'utilisateurs Db2 avant la connexion à un serveur Db2 local», à la page 140
   Installez ensuite le serveur Cloud APM. Pour des instructions, voir :
   «Téléchargement et installation du serveur», à la page 141

   Remarque : Si le serveur Cloud APM source est configuré pour utiliser un serveur Db2 distant et que vous suivez l'option 2.c., vous devez installer le serveur Cloud APM cible pour utiliser un serveur Db2 local afin que le processus d'installation ne modifie pas les bases de données existantes. Une fois l'installation du serveur Cloud APM terminée, reconfigurez le serveur Cloud APM cible pour utiliser les mêmes bases de données que le serveur Cloud APM source en suivant les étapes décrites dans les rubriques ci-dessous :
   a. «Catalogage des bases de données Db2 après modification du serveur Db2», à la page 1085
   b. «Mise à jour de la configuration du serveur Cloud APM pour prendre en compte les modifications du serveur Db2», à la page 1087. Veillez à définir le mot de passe itmuser sur le mot de passe itmuser sur le serveur Db2 distant lorsque vous exécutez cette procédure.
   c. Voir «Modification d'un mot de passe», à la page 1076 pour définir le mot de passe pour l'utilisateur de l'instance `db2apm` afin qu'il corresponde au mot de passe de l'instance Db2 sur votre

serveur Db2 distant. Le script `restore.sh` peut alors déterminer le mot de passe de l'instance Db2 distante lors de l'exécution d'une reprise après incident.

Résultats

L'installation du serveur Cloud APM cible est terminée et ce dernier est prêt à être utilisé pour la reprise.

Que faire ensuite

Effectuez la reprise en utilisant un fichier de sauvegarde récent. Pour obtenir des instructions, voir «Restauration des composants pour la reprise après incident», à la page 1109.

Exploration des API

Utilisez les API IBM Cloud Application Performance Management pour créer des scripts afin d'automatiser l'intégration de votre environnement IBM Cloud Application Performance Management, Private.

A partir de l'offre de service gérée par API Cloud APM de l'Explorateur d'API sous IBM developerWorks, vous pouvez accéder aux API Resource Group Management Service, Threshold Management Service et Role-Based access control Service disponibles.

Procédure

1. Ouvrez l'Explorateur d'API dans votre navigateur : https://developer.ibm.com/api.
2. Sélectionnez la mosaïque de l'API IBM Cloud Application Performance Management.
3. Cliquez sur **Documentation** à gauche de la fenêtre Explorateur d'API.
4. Sélectionnez l'API spécifique.
5. Sélectionnez la sous-section pour développer la liste des opérations API.
6. Sélectionnez une opération API pour plus de détails.
7. Sélectionnez l'un des langages (tels que shell ou curl) en haut de la page de l'API Explorer pour afficher un exemple de demande.

Que faire ensuite

Pour plus d'informations sur la manière d'obtenir votre jeton d'accès et d'exécuter des opérations API, voir les rubriques suivantes :

«Accès et utilisation de l'API Role-Based Access Control Service», à la page 1037

«Utilisation de l'API Resource Group Management Service», à la page 1014

«Utilisation de l'API Threshold Management Service», à la page 1017

Ajustement de la valeur de délai de la console

Lorsque la console Cloud APM est démarrée, un jeton LTPA (Lightweight Third-Party Authentication) et un jeton d'ID OIDC (OpenID Connect) sont attribués pendant le processus de connexion.

Le délai d'expiration par défaut du jeton LTPA est de 200 minutes, au-delà duquel vous êtes automatiquement déconnecté. Vous pouvez modifier la valeur de délai afin de répondre à vos besoins professionnels.

Avant de commencer

Le délai d'expiration du jeton d'ID OIDC est de 120 minutes, au-delà duquel vous revenez à la page de connexion. Le délai d'expiration du jeton LTPA est configurable, au contraire de celui du jeton d'ID OIDC, qui ne l'est pas. Aussi, les implications sont comme suit :

- Si OIDC est activé pour Cloud APM (comportement par défaut), le fait de définir l'expiration du jeton LTPA sur une valeur supérieure à 120 minutes n'a aucune incidence puisque le jeton d'ID OIDC expire au bout de ce laps de temps et les utilisateurs de la console reviennent à la page de connexion. Par conséquent, lorsqu'OIDC est activé, vous pouvez configurer la console de sorte que le délai d'attente expire avant celui du jeton d'ID OIDC en définissant l'expiration du jeton LTPA sur une valeur inférieure à 120 minutes.
- Vous pouvez désactiver OIDC afin d'augmenter le délai de la console. Suivez les étapes décrites dans «Désactivation de l'authentification OpenID Connect pour la console Cloud APM», à la page 922, puis l'étape 10, à la page 925 (spécifiez le nom de domaine du serveur Cloud APM pour l'attribut **ssoDomainNames**) à l'étape 13, à la page 925 de «Activation de la connexion unique entre Cloud APM et Tivoli Common Reporting», à la page 923. Vous pouvez suivre ces étapes même si vous n'effectuez pas l'intégration à un autre produit, tel que Tivoli Common Reporting ou Dashboard Application Services Hub.

Remarque : Vous devez installer le correctif temporaire 5 ou ultérieur du serveur Cloud APM V8.1.4.0 si vous suivez cette procédure afin que la valeur de délai dans les fichiers `user-exit.xml` soit utilisée. (Le fichier `user-exit.xml` se substitue à `server.xml`.) Le correctif temporaire peut être installé avant ou après l'exécution de la procédure. Vous pouvez télécharger ce correctif pour serveur Cloud APM V8.1.4 depuis IBM Fix Central.

Procédure

Sur le système sur lequel le serveur Cloud APM est installé, procédez comme suit pour modifier la valeur d'expiration du jeton LTPA dans les fichiers `user-exit.xml` :

1. Ouvrez le fichier *rép_install*`/wlp/usr/servers/apmui/user-exit.xml` dans un éditeur de texte.
2. Si l'élément XML ltpa expiration n'existe pas dans le fichier `user-exit.xml`, copiez-le depuis `server.xml` vers `user-exit.xml`.
3. Modifiez le paramètre `<ltpa expiration="200m" />`, puis remplacez la valeur d'expiration LTPA par un entier positif suivi d'une unité de temps exprimée en heures (h) ou minutes (m). Par exemple, `"8h"` indique 8 heures. La valeur maximale prise en charge pour le délai est 35791394 minutes (m) ou 596523 heures (h), qui correspond à 24 jours environ. Utilisez la lettre "h" ou "m" en minuscules. Si vous utilisez une majuscule ("H" par exemple) ou une autre lettre ("d" par exemple), votre connexion est supprimée sans préavis par le composant Liberty du serveur Cloud APM.
4. Supprimez l'élément XML ltpa du fichier *rép_install*`/wlp/usr/servers/apmui/server.xml`.
5. Ouvrez le fichier *rép_install*`/wlp/usr/servers/uview/user-exit.xml` dans un éditeur de texte.
6. Ajoutez l'élément XML ltpa expiration s'il n'existe pas, puis définissez sa valeur afin qu'elle corresponde à la valeur d'expiration dans le fichier *rép_install*`/wlp/usr/servers/apmui/user-exit.xml` (étape 3).
7. Supprimez l'élément XML ltpa du fichier *rép_install*`/wlp/usr/servers/uview/server.xml`.
8. Sauvegardez et fermez les deux fichiers `user-exit.xml`.

Résultats

La prochaine fois que les utilisateurs se connecteront au serveur Cloud APM, ils seront déconnectés après l'expiration du délai d'attente.

Tâches associées:

«Verrouillage de la console Cloud APM», à la page 1172
Vous pouvez verrouiller temporairement votre session de travail sans devoir vous déconnecter de la

console Cloud APM.

Information associée:

«Fonction d'abonnement d'agent», à la page 1121

Configuration avancée

Utilisez la page Configuration avancée pour contrôler les paramètres de communications et les fonctions avancées, par exemple l'acheminement d'événement.

Après avoir cliqué sur **Configuration système** > **Configuration avancée**, les catégories de configuration ci-dessous s'affichent sur la page Configuration avancée.

Intégration de l'interface utilisateur

Pour les produits qui s'intègrent à la console Cloud APM, vous pouvez ajouter ou éditer l'URL permettant de lancer l'application intégrée. Les zones sont alimentées avec les URL définies lors de la procédure de configuration de l'intégration.

- L'**URL de Cognos Reporting** permet de lancer IBM Cognos Viewer pour afficher les rapports Cloud APM via **Rapport** > **Gérer des rapports** et **Actions** > **Rapports de lancement**.

  Le format de l'**URL de Cognos Reporting** doit être le suivant :

  `https://`*`nomhôte_serveur_générationrapports`*`:`*`port`*`/tarf/servlet/dispatch/secured`

  Pour afficher des rapports avec Tivoli Common Reporting 3.1.1 ou version ultérieure, le format de l'**URL de Cognos Reporting** doit être le suivant :

  `https://`*`nomhôte_serveur_générationrapports`*`:`*`port`*`/tarf/servlet/reporting/secured`Pour plus d'informations, voir «Rapports», à la page 1172.
- **Cognos Reporting Requires XSS Validation** permet de reformater l'URL pour que le rapport Cognos réussisse la validation XSS. Définissez cette zone sur `True` si votre configuration a activé Cognos Application Firewall (CAF) et la vérification XSS tierce. Valeur par défaut : `False`. Pour plus d'informations, voir «Intégration à Tivoli Common Reporting», à la page 917.
- L'**URL de Log Analysis** permet de lancer IBM Operations Analytics - Log Analysis pour effectuer des recherches dans les journaux d'application du Tableau de bord d'Application Performance. Pour plus d'informations, voir «Recherche dans les fichiers journaux», à la page 1127.
- **Activer les événements sous-noeud**, pour les agents avec sous-noeuds, contrôle si les sous-noeuds apparaissent dans l'onglet Evénements. Lorsque les événements de sous-noeud sont activés, le noeud et le sous-noeud pour lesquels un événement a été ouvert s'affichent. En particulier, si vous voulez afficher les situations de surveillance des fichiers journaux dans l'onglet Evénements, vous devez vérifier que les événements de sous-noeud sont activés. Valeur par défaut : `False`.
- **Dashboard Refresh Rate** contrôle la fréquence d'actualisation automatique du Tableau de bord d'Application Performance. Vous pouvez ajuster le paramètre sur une valeur comprise entre 1 et 60 minutes. Le paramètre affecte le statut des ressources qui s'affiche dans le navigateur et dans l'onglet Présentation des statuts. Il n'a aucun impact sur les entrées de l'onglet Evénements. Valeur par défaut : 1 minute.

Gestionnaire d'événements

Le gestionnaire d'événements contrôle le flux (transféré au Protocole SMTP (Simple Mail Transfer Protocol)), le stockage des événements reçus et la configuration de la notification par e-mail. Si vous entrez une valeur pour Adresses e-mail cible, Compte de messagerie d'envoi, Mot de passe du compte de messagerie d'envoi et Adresse du serveur SMTP, un e-mail est envoyé pour chaque événement d'ouverture, de fermeture et d'arrêt.

Si vous configurez le réexpéditeur SMTP afin qu'il utilise SSL, vous devez ajouter le certificat de l'autorité de certification signataire du serveur SMTP au fichier de clés du serveur Cloud APM. Ajoutez le certificat de l'autorité de certification au fichier de clés par défaut en utilisant la commande keytool de la machine JVM :

```
rép_install/java/jre/bin/keytool -importcert\
-noprompt \
-alias votre_alias_cert_AC \
-file chemin_vers_votre_fichier_cert_AC (*.cer)
 -keystore /rép_install/wlp/usr/servers/min/resources/security/key.jks \
-storepass ccmR0cKs! \
-storetype jks \
-trustcacerts
```

Pour visualiser un exemple de courrier électronique, voir «E-mail d'événement», à la page 1122.

- **Durée du cache d'événement** détermine le nombre de minutes pendant lesquelles les événements sont conservés dans le cache local, de 10 minutes au minimum jusqu'à 480 minutes (8 heures). Si la liste d'événements est longue, essayez de réduire le nombre de minutes de conservation. Ou, pour afficher les événements survenus au cours d'une période plus longue, augmentez le nombre de minutes. Valeur par défaut : `60` minutes.
- **Heures avant la fermeture des événements purs** détermine combien de temps il faut garder un événement pur ouvert avant de le fermer. Valeur par défaut : `24` heures.
- **L'événement de réinitialisation principal** contrôle s'il convient d'envoyer un événement de réinitialisation principal pour effacer les événements échantillonnés reçus précédemment après le redémarrage de l'agent de surveillance. Si les notifications par courrier électronique sont configurées, vous recevez également un e-mail (voir un exemple sur «Evénement de réinitialisation principal après le redémarrage de l'agent», à la page 1124). Valeur par défaut : `True`.
- **Port de la fonction d'intégration d'événements** indique le numéro de port à utiliser pour recevoir les événements de fonction d'intégration d'événements d'Operations Analytics - Predictive Insights. Si vous ne spécifiez pas de numéro de port pour une cible de fonction d'intégration d'événements dans la zone **Cible(s) d'événement de fonction d'intégration d'événements**, la valeur de la zone **Port de la fonction d'intégration d'événements** est également utilisée comme numéro de port lors de la transmission d'événements à cette cible de fonction d'intégration d'événements. Valeur par défaut : `9998`.
- **Cible(s) d'événement de fonction d'intégration d'événements** spécifie la liste des noms d'hôte ou adresses IP et numéros de port vers lesquels tous les événements de fonction d'intégration d'événements sont réacheminés. Par exemple, si vous transmettez les événements à Netcool/OMNIbus Probe for Tivoli EIF, entrez le nom d'hôte qualifié complet ou l'adresse IP de l'ordinateur sur lequel la sonde est installée, suivi du numéro de port du récepteur. Séparez chaque nom d'hôte et numéro de port par un deux points (:), et séparez chaque nom d'hôte par une virgule (,), par exemple `9.87.65.111:8989,localhost:9090,myhostname.en.ibm.com`. Si vous n'incluez pas de numéro de port avec le nom d'hôte du récepteur d'événements EIF, la valeur de la zone **Port de la fonction d'intégration d'événements** est utilisée. Les adresses IPv6 sont pas prises en charge pour la transmission EIF.
- **Adresses e-mail cibles** indique les adresses électroniques vers lesquelles sont acheminés les événements. Séparez chaque adresse par une virgule (,), comme `annette@ibm.com,jim@ibm.com,owen@ibm.com`.
- **Sending Email Account** est utilisé pour l'authentification quand **Utiliser SSL** est défini sur `True`. Il s'agit de l'adresse de courrier électronique pour envoyer un événement d'e-mail SMTP et cet élément apparaît comme l'expéditeur de l'e-mail.
- **Sending Email Account Password** est le mot de passe associé au compte d'expédition d'e-mail lorsque **Utiliser SSL** est défini sur `True`.
- **Adresse du serveur SMTP** est le nom d'hôte qualifié complet du serveur SMTP utilisé pour l'envoi d'événements sous la forme d'e-mails, comme `smtp.gmail.com`.

- **Utiliser SSL** détermine s'il convient d'utiliser SSL comme mécanisme de transport SMTP (Simple Mail Transfer Protocol). Si vous définissez cette zone sur `True`, renseignez les zones **Sending Email Account** et **Sending Email Account Password**, qui sont requises pour l'authentification. Valeur par défaut : `False`.
- **Port SMTP** est le numéro de port à utiliser pour l'envoi d'e-mails SMTP. Valeur par défaut : `25`.
- **Port SMTP SSL** est le numéro de port à utiliser pour envoyer un e-mail SMTP à l'aide du protocole SSL (Secure Socket Layer). Valeur par défaut : `465`.
- **Noeud final d'API de notification d'alerte** correspond à l'URL associée à l'API de notification d'alerte utilisée pour traiter les notifications d'alerte. Pour afficher l'URL, ouvrez l'interface utilisateur d'Alert Notification et cliquez sur **Manage API Keys** et sur l'icône d'information. Copiez l'URL d'API affichée et collez-la dans cette zone.
- **Alert Notification API Key** représente la clé créée dans l'interface utilisateur d'Alert Notification. Cette clé d'API est associée au mot de passe d'API entré avec ce paramètre de configuration. Pour générer la clé de l'API Alert Notification, voir Gestion des clés d'API
- **Alert Notification API Password** représente le mot de passe associé à la clé entrée avec le paramètre de configuration **`Alert Notification API Key`**. Pour générer le mot de passe de l'API Alert Notification, voir Gestion des clés d'API
- **Alert Notification for ITMv6** est l'option qui permet d'activer les événements Alert Notification for ITMv6 en définissant la valeur `True`. Valeur par défaut : `False`

Vous pouvez utiliser Alert Notification au lieu de la fonction de messagerie du gestionnaire d'événements pour contrôler les personnes notifiées pour des événements différents et leur mode de notification. Pour plus d'informations, voir «Intégration à Alert Notification», à la page 908.

Si vous transmettez des événements à un récepteur EIF (Event Integration Facility), vous pouvez personnaliser les emplacements EIF de sorte à ajouter un attribut à l'événement EIF. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1007. Pour plus d'informations sur la transmission de vos événements au gestionnaire d'événements IBM Netcool/OMNIbus, reportez-vous à la rubrique Intégration à Netcool/OMNIbus (cloud) ou Intégration à Netcool/OMNIbus (sur site) dans le «Intégration à Netcool/OMNIbus», à la page 905.

Configuration MongoDB

Configurez la base de données MongoDB.

- **Nom d'hôte** est le nom d'hôte du système dans lequel s'exécute MongoDB. Valeur par défaut : `localhost`.
- **Numéro de port** est le numéro de port de la base de données Mongo. Valeur par défaut : `27000`.
- **Taille des lots** est le nombre de documents AAR traités et insérés par MongoDB ETL dans le document MongoDB au cours d'une seule insertion par lot. Valeur par défaut : `100`.
- **Attente dans batch** est le délai d'attente avant l'insertion d'un lot incomplet de documents AAR dans le document MongoDB, depuis que le dernier message a été traité. Valeur par défaut : `10` secondes.

Configuration centrale d'agent

Les paramètres sont des informations obligatoires utilisées par le serveur Cloud APM pour configurer Central Configuration Services. Le composant Central Configuration Services permet de distribuer les événements, les seuils et les paramètres des données historiques aux agents de surveillance. Chaque agent de même type reçoit les mêmes seuils et paramètres.

- **Substitution du nom d'hôte** est une substitution facultative du nom d'hôte ou de l'adresse IP de Central Configuration Services si la valeur du serveur n'est pas correcte. Par défaut, l'adresse IP ou le nom d'hôte que vous avez indiqué(e) lors de la configuration des packages d'agent est utilisé(e).

- L'option **Changer l'intervalle de vérification** contrôle la fréquence, en minutes, utilisée par les agents de surveillance pour demander les détails de configuration du serveur. Valeur par défaut : `5` minutes.
- **Protocole** indique si HTTP ou HTTPS est le protocole utilisé pour la communication avec l'agent de surveillance. Si la variable *APM_SECURE_COMMUNICATION* a été définie sur `Y` avant l'installation du serveur, cette zone est définie sur HTTPS pour une connexion sécurisée. Pour plus d'informations, voir «Définition des communications HTTP ou HTTPS», à la page 128. Valeur par défaut : `HTTP`.
- **Port HTTP** détermine le port à utiliser pour les communications HTTP. Valeur par défaut : `80`.
- **Port HTTPS** détermine le port à utiliser pour les communications HTTPS sécurisées. Valeur par défaut : `443`.

Entrepôt de données

Ces paramètres peuvent être ajustés pour améliorer les performances :

- **Taille des lots** est le nombre de lignes à inclure dans une transaction de base de données unique. Valeur par défaut : `100` lignes.
- **Intervalle entre les lots** est l'intervalle entre l'envoi des données à la base de données pour autoriser leur insertion. Valeur par défaut : `10` secondes.

Configurez une base de données externe pour l'entrepôt de données.

- **Facultatif, JDBC** peut être utilisé pour définir des propriétés supplémentaires, telles que le chiffrement. Le format est `key=value`, une entrée par ligne.

Configuration Kafka

Le courtier de messages Kafka possède des paramètres de configuration prédéfinis. Conservez la valeur par défaut de ces paramètres à moins que le support IBM ne vous demande de les modifier.

- **Taille des lots de fournisseur** désigne le nombre de messages envoyés par lots chez le fournisseur avant attribution au gestionnaire d'événements. Valeur par défaut : `200` messages.
- **Attente dans batch de fournisseur** désigne le délai d'attente du fournisseur. Valeur par défaut : `5` secondes.
- **Taille des lots de consommateur** désigne le nombre d'enregistrements à inclure dans une seule transaction de base de données. Valeur par défaut : `100` enregistrements.
- **Attente dans batch de consommateur** correspond au délai d'attente entre les envois de lots de données à la base de données pour autoriser les insertions par lots. Si la **Taille des lots de consommateur** n'est pas atteinte au cours de cet intervalle, les données sont vidées. Valeur par défaut : `10` secondes.
- **Nombre d'unités d'exécution de consommateur** désigne le nombre d'unités d'exécution de consommateur. Valeur par défaut : `2` unités d'exécution.

Service d'analyse de suivi

Paramètres utilisés pour le service d'analyse de suivi. Les paramètres s'appliquent uniquement à l'offre Cloud APM, Advanced Private et si vous configurez le suivi des transactions dans votre environnement.

- La **Taille du pool de connexions** correspond au nombre de connexions Db2 simultanées que le service d'analyse du suivi maintient dans le pool de connexions pour la demande des «*N* premiers». Augmentez cette valeur si vous êtes confronté à des périodes pour lesquelles le délai est lent en raison d'un nombre important d'utilisateurs simultanés de la console Cloud APM. Valeur par défaut : `10`.
- Les **Pseudo-noeuds** activent la visualisation des services qui ne sont pas instrumentés. Valeur par défaut : `True`.
- Le **Délai d'attente de requête en secondes** est le nombre de secondes nécessaires à chaque demande des "*N* premiers" (où *N* est un nombre comme dans «5 premiers» ou «10 premiers») avant que le délai d'attente soit dépassé. La valeur du délai d'attente peut être augmentée pour

les applications dont la charge de travail est plus élevée et dont les périodes de délai attendues sont plus importantes. Valeur par défaut : 120 secondes.

- En général, le paramètre **Réoptimisation des requêtes DB2 activée** n'a pas à être modifié. Ce paramètre affecte l'optimiseur de requêtes Db2. Dans certains environnements, la désactivation de l'optimiseur peut améliorer les performances pour certains ensembles de transactions. Valeur par défaut : False.

Fonction d'abonnement d'agent

Agent Subscription Facility inclut l'interface REST (Representative State Transfer) de l'agent et le serveur HTTP de Central Configuration Services. L'interface REST est utilisée par les agents et les collecteurs de données pour envoyer les données de surveillance conservées sur le serveur Db2 et les événements de seuil. Le serveur HTTP de Central Configuration Services gère les demandes des agents pour les fichiers de configuration, tels que les définitions de seuil. Utilisez ces paramètres pour configurer les communications entre la fonction d'abonnement d'agent et le serveur Cloud APM.

- **Limite du nombre d'interrogations manquées (signal de présence rapide)** désigne le nombre maximal de fois où un agent de surveillance, avec un intervalle entre les signaux de présence inférieur ou égal à 60 secondes, ne parvient pas à se connecter avant d'être marqué comme étant hors ligne. Valeur par défaut : 30 intervalles.
- **Limite du nombre d'interrogations manquées (signal de présence lent)** désigne le nombre maximal de fois où un agent de surveillance, avec un intervalle entre les signaux de présence supérieur à 60 secondes, ne parvient pas à se connecter avant d'être marqué comme étant hors ligne. Valeur par défaut : 3 intervalles.
- **Délai d'expiration de la transaction** désigne la durée, en secondes, pendant laquelle le serveur attend une réponse à une demande. Valeur par défaut : 120 secondes.
- **Compte de régulation** désigne le nombre de demandes adressées par le serveur à l'agent de surveillance pour un rappel après un court délai avant de l'autoriser à fermer la connexion. Valeur par défaut : 5.
- **Délai de régulation** désigne le temps en millisecondes, pendant lequel un agent de surveillance attend avant d'adresser une demande de travail supplémentaire au serveur. Valeur par défaut : 600 000 millisecondes (10 minutes).
- **Délai avant suppression d'un système hors ligne** détermine le nombre de minutes d'attente avant le retrait de l'affichage d'un système géré hors ligne. Dans le Tableau de bord d'Application Performance, les systèmes gérés autonomes sont indiqués par l'indicateur de statut inconnu . Le système géré reste affiché, même si vous désinstallez l'agent, jusqu'à ce que le délai soit terminé. Pour plus d'informations, voir «Affichage et suppression des agents en ligne», à la page 1151. Valeur par défaut : 5760 minutes (4 jours).

Activation des seuils

Vos agents de surveillance contiennent tous un ensemble de seuils prédéfinis qui sont activés et démarrés avec l'agent. Ces seuils prédéfinis sont affectés au groupe de ressources système par défaut pour l'agent.

- L'option **Sélectionnez une action afin de définir la règle des seuils de meilleure pratique prédéfinis** contrôle si les seuils prédéfinis pour vos ressources gérées sont activés ou désactivés par défaut. Définissez la zone sur **Désactiver tout** si vous ne voulez pas exécuter les seuils prédéfinis. Le paramètre **Désactiver tout** supprime l'affectation du groupe de systèmes de tous les seuils prédéfinis. Un seuil auquel aucun groupe n'est affecté n'est distribué à aucun système surveillé et reste arrêté jusqu'à ce qu'il soit distribué à un groupe de ressources. Si vous décidez par la suite d'activer les seuils prédéfinis, définissez la zone sur **Activer tout**.

Pour plus d'informations sur les seuils prédéfinis et les seuils personnalisés, voir «Informations de référence», à la page 990 et «Exemples de seuils désactivés», à la page 992.

E-mail d'événement

Utilisez les zones du Gestionnaire d'événements de la page Configuration avancée pour configurer la notification d'événements par courrier électronique à une liste de destinataires.

Email for open event
Lorsqu'une condition de seuil est vérifiée, un événement est ouvert et le message électronique envoyé par le serveur Cloud APM contient les attributs de base qui s'appliquent à tous les événements, ainsi que les attributs de la première ligne du jeu de données correspondant à la condition de seuil. L'attribut situation_status possède la valeur Y pour les événements ouverts.

Email for close events
Lorsqu'une condition de seuil n'est plus vérifiée, un événement de fermeture est généré. Le message électronique des événements de fermeture ne contient que les attributs de base qui s'appliquent à tous les événements d'agent et la valeur de l'attribut situation_status est N. Les attributs de l'agent ne sont pas inclus dans ces messages électroniques car la condition de seuil n'est pas remplie.

Email for stop event
Lorsqu'un seuil est arrêté, un événement d'arrêt est généré. Le message électronique des événements d'arrêt ne contient que les attributs de base qui s'appliquent à tous les événements d'agent et la valeur de l'attribut situation_status est P. Les attributs de l'agent ne sont pas inclus dans ces messages électroniques car la condition de seuil n'est pas remplie.

Un seuil est arrêté pour un agent si vous supprimez la définition de seuil ou que vous modifiez l'une des définitions de seuil distribuées à l'agent.

Les exemples suivants montrent un e-mail pour un événement d'ouverture :

```
From:    noreply@apm.ibmserviceengage.com
To:         tester@us.ibm.com
Date:    10/25/2017 01:56 PM
Subject:    Linux_Disk_Space_Low on nc049048:LZ (Notification)
Le text ci-dessous répertorie les informations reçues de l'agent qui a déclenché cet événement.
Les valeurs IP et Agent identifient l'agent qui a détecté l'événement.
Les valeurs Description et Severity indiquent le nom de la définition de seuil et sa gravité.
Sous la description se trouvent toutes les paires attribut/valeur présentes dans l'événement, dans leur forme brute.
    Server IP  : 10.107.76.230 (SIDR26APAP1BLUE.test.ibm.com)
    Agent IP   : 9.42.49.48
    Agent      : nc049048:LZ
    Severity   : warning
    Description: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                 AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups='*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      adapter_host=nc049048.tivlab.raleigh.ibm.com
      apm_hostname=SIDR26APAP1BLUE.test.ibm.com
      appl_label=A:P:S
      date=01/25/2017
      disk_free=5843
      disk_free_percent=20
      disk_name=/dev/sda2
      disk_used=22676
      disk_used_percent=80
      file_system_status=2
      file_system_status_enum=Up
      fqhostname=nc049048.test.ibm.com
      fs_type=ext4
      hostname=nc049048.test.ibm.com
      identifier=Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      inodes_free=1721587
      inodes_free_percent=88
      inodes_used=232477
      inodes_used_percent=12
```

```
      integration_type=U
      mount_options=rw
      mount_point=/
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type != nfs
     AND FS_Type != iso9660 ]'
      origin=9.42.49.48
      severity=WARNING
      situation_displayitem=/
      situation_eventdata='disk_name=/dev/sda2;inodes_used_percent=12;mount_options=rw;fs_type=ext4;
     system_name=nc049048:LZ;mount_point=/;disk_used_percent=80;disk_free=5843;file_system_status_enum=Up;
     size=30040;disk_used=22676;inodes_used=232477;disk_free_percent=20;file_system_status=2;
     total_inodes=1954064;inodes_free=1721587;timestamp=1170125135553000;inodes_free_percent=88;~'
      situation_name=Linux_Disk_Space_Low
      situation_origin=nc049048:LZ
      situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      situation_status=Y
      situation_thrunode=nc049048:LZ
      situation_time='01/25/2017 13:55:55.000'
      situation_type=S
      size=30040
      source='ITM Agent: Private Situation'
      sub_origin=/
      sub_source=nc049048:LZ
      system_name=nc049048:LZ
      timestamp=1170125135553000
      tmz_diff=18000
      total_inodes=1954064
Pour vous désabonner de ces e-mails, connectez-vous à la console Cloud APM et
retirez votre adresse e-mail de
la liste des adresses e-mail cible dans la catégorie Gestionnaire
d'événements de la page Configuration avancée.
```

L'exemple suivant montre un e-mail pour un événement de fermeture.

```
From:    noreply@apm.ibmserviceengage.com
To:      tester@us.ibm.com
Date:    01/25/2017 02:01 PM
Subject:    Linux_Disk_Space_Low on nc049048:LZ (Closed)
Le text ci-dessous répertorie les informations reçues de l'agent qui a déclenché cet événement.
Les valeurs IP et Agent identifient l'agent qui a détecté l'événement.
Les valeurs Description et Severity indiquent le nom de la définition de seuil et sa gravité.
Sous la description se trouvent toutes les paires attribut/valeur présentes dans l'événement, dans leur forme brute.
    Server IP  : 10.107.76.230 (SIDR26APAP1BLUE-12f.test.ibm.com)
    Agent IP   : 9.42.49.48
    Agent      : nc049048:LZ
    Severity   : warning
    Description: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                 AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups='*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      adapter_host=nc049048.tivlab.raleigh.ibm.com
      apm_hostname=SIDR26APAP1BLUE-12f.test.ibm.com
      appl_label=A:P:S
      date=01/25/2017
      fqhostname=nc049048.test.ibm.com
      hostname=nc049048.test.ibm.com
      identifier=Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      integration_type=U
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type != nfs
     AND FS_Type != iso9660 ]'
      origin=9.42.49.48
      severity=WARNING
      situation_displayitem=/
      situation_eventdata=~
      situation_name=Linux_Disk_Space_Low
      situation_origin=nc049048:LZ
```

```
      situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      situation_status=N
      situation_thrunode=nc049048:LZ
      situation_time='01/25/2017 14:00:55.000'
      situation_type=S
      source='ITM Agent: Private Situation'
      sub_origin=/
      sub_source=nc049048:LZ
      tmz_diff=18000
Pour vous désabonner de ces e-mails, connectez-vous à la console Cloud APM et
retirez votre adresse e-mail de
la liste des adresses e-mail cible dans la catégorie Gestionnaire
d'événements de la page Configuration avancée.
```

Evénement de réinitialisation principal après le redémarrage de l'agent

Si la zone **Evénement de réinitialisation principal** est défini sur True, un courrier électronique similaire à celui montré dans l'exemple est envoyé aux destinataires de la zone **Adresses e-mail cible** chaque fois que l'agent de surveillance est redémarré.

```
From: ipm@ibm.com
To: Andrea Chiavegatto@mycompany.com,
Date: 06/20/2017 03:47 PM
Subject: Agent MyHost:LZ has restarted.
Le text ci-dessous répertorie les informations reçues de l'agent qui a déclenché cet événement.
Les valeurs IP et Agent identifient l'agent qui a détecté l'événement.
Les valeurs Description et Severity indiquent le nom de la définition de seuil et sa gravité.
Sous la description se trouvent toutes les paires attribut/valeur présentes dans l'événement, dans leur forme brute.
    IP         : 9.40.11.111
    Agent      : MyHost:LZ
    Severity   : MINOR
    Description: Agent MyHost:LZ has restarted.
       ITM_Generic
       appl_label='A:P:S'
       date='06/20/2017'
       fqhostname='MyHost.tivlab.raleigh.ibm.com'
       hostname='MyHost.tivlab.raleigh.ibm.com'
       master_reset_flag='R'
       msg='Agent MyHost:LZ has restarted.'
       origin='9.99.22.133'
       severity='MINOR'
       situation_name='**'
       situation_origin='MyHost:LZ'
       situation_origin_uuid='f69a1b769b77.22.02.09.62.16.85.05.32'
       situation_status='N'
       situation_time='06/20/2017 15:46:36.000'
       source='ITM Agent: Private Situation

Pour vous désabonner de ces e-mails, connectez-vous à la console Cloud APM et
retirez votre adresse e-mail de
la liste des adresses e-mail cible dans la catégorie Gestionnaire
d'événements de la page Configuration avancée.
```

Chapitre 14. Utilisation des tableaux de bord

Sélectionnez **Performance** > **Tableau de bord d'Application Performance** pour obtenir une présentation complète du statut de vos applications. Vous pouvez effectuer une exploration en aval de la vue la plus générale à la vue détaillée des mesures, dans le même écran.

Utilisez les outils disponibles dans les tableaux de bord pour examiner les conditions ayant le statut critique ou avertissement dans votre environnement, créer des vues de mesures supplémentaires, ainsi que pour exécuter des actions telles que des recherches dans les journaux de trace et la comparaison de mesures dans le temps.

Toutes mes applications - Tableau de bord d'Application Performance

Le Tableau de bord d'Application Performance présente le récapitulatif des statuts de vos domaines surveillés dans **Toutes mes applications**.

Une *zone récapitulative* est affichée pour chaque application définie par l'utilisateur, comme par exemple «Inventory Management», et pour les applications prédéfinies, «Mes composants» ou «Mes transactions» si votre environnement inclut de telles applications. A partir des zones récapitulatives ou du navigateur, explorez en aval chaque application et ses constituants afin d'en voir les mesures détaillées.

Au fur et à mesure que vous sélectionnez des éléments, le chemin correspondant s'affiche au-dessus du titre de l'élément sélectionné et vous pouvez cliquer sur l'un des liens de chemin pour revenir à cette vue. A partir de n'importe quelle page de la console Cloud APM, vous pouvez cliquer sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**. Visualisez les domaines qui vous intéressent en les sélectionnant dans le navigateur ou en cliquant dans une zone récapitulative pour accéder au niveau suivant.

Zones récapitulatives

Toutes mes applications comporte une zone récapitulative pour chaque application définie. Des indicateurs définissent la gravité de statut la plus élevée pour l'application dans la barre de titre et pour chaque groupe dans la zone récapitulative. Les groupes prédéfinis disponibles sont les suivants, selon les produits de surveillance inclus dans l'application définie :

Composants contient un sous-groupe pour chaque type d'agent de surveillance prenant en charge votre application

Transactions peut inclure Transactions utilisateur final et Transactions synthétiques

De plus, chaque zone récapitulative inclut la zone **Evénements**, qui affiche la gravité de l'événement dont la gravité est la plus élevée ayant été ouvert pour l'application. Vous pouvez cliquer sur le lien Evénements pour rechercher tous les événements ouverts (voir «Statut de l'événement», à la page 1156).

 . Cliquez sur la barre de titre d'une zone récapitulative pour ouvrir l'onglet Présentation des statuts de l'application. Ou cliquez sur l'une des icônes de zone récapitulative pour ouvrir l'onglet Présentation des statuts pour le groupe Composants ou le sous-groupe Utilisateurs ou Transactions, ou pour ouvrir l'onglet Evénements pour le groupe ou le sous-groupe d'applications.

Vous pouvez réduire les cases récapitulatives et les filtrer en cochant ou en désélectionnant des cases :

- Pour afficher seulement les barres de titre récapitulatives afin de faciliter le défilement dans vos applications définies, décochez la case **Afficher les détails**.

© Copyright IBM Corp. 2015, 2018

- Pour filtrer les zones récapitulatives sur le statut de gravité à masquer, désélectionnez la case d'un compteur comme  . La case à cocher d'une gravité sans événements est désélectionnée. Par exemple, dans ce graphique, les filtres pour Critique et Normal sont activés ; Avertissement et Inconnu sont désactivés car ils ont un nombre égal à 0 :


Rechercher

Utilisez la zone Rechercher pour rechercher les entrées de journal de la dernière heure qui contiennent le texte saisi. Vous pouvez cliquer sur  pour afficher les résultats d'une autre plage de temps. Le texte à rechercher est comparé aux entrées de journal associées à la sélection du navigateur et les correspondances s'affichent dans un nouvel onglet ou une nouvelle fenêtre de navigateur. Pour plus d'informations, voir «Recherche dans les fichiers journaux», à la page 1127. La fonction de recherche est fournie par IBM Operations Analytics - Log Analysis.

Actions

Le menu **Actions** comporte des options pour copier l'URL, pointant vers le journal de tableau de bord, et définir une trace pour le traitement des incidents. Pour plus d'informations, voir «Copie de l'URL du tableau de bord», à la page 1170 et «Définition d'une trace», à la page 1170.

Utilisez l'option de **journal de tableau de bord** pour passer en revue la liste des tableaux de bord d'agent mis à jour depuis le dernier redémarrage du serveur.

Lorsque le tableau de bord de base **Toutes mes applications** ou l'une des applications est sélectionné, le menu Actions inclut l'option **Rapports de lancement** pour vous aider à analyser les tendances en matière d'utilisation et de performance si les rapports Cognos sont disponibles et si votre environnement comprend Tivoli Common Reporting. Pour plus d'informations, voir «Rapports», à la page 1172.

Lorsque le groupe **Composants** est sélectionné, à partir de la section **Groupes** du navigateur ou d'une zone récapitulative, le menu **Actions** contient une option d'**édition** permettant d'éditer le tableau de bord de présentation des statuts des composants. L'option **Editer** est disponible uniquement si l'utilisateur dispose des droits de modification du tableau de bord Performance Management et des droits de création d'applications. Pour plus d'informations, voir «Edition des widgets de groupe du tableau de bord Composants», à la page 1137.

Aide

Ouvrez l'aide contextuelle pour obtenir une brève description du tableau de bord actuel, avec les liens suivants : **En savoir plus** ouvre l'intégralité de la rubrique de tableau de bord dans le système d'aide local Cloud APM ; **Visite guidée du tableau de bord** lance la visite guidée du tableau de bord d'IBM Cloud APM, qui présente une brève description des éléments du tableau de bord tout en présentant ses différentes fonctions.

Navigateur

Le navigateur affiche une hiérarchie des applications, ainsi que de leurs utilisateurs, transactions et composants, qui reflète leur organisation. Le navigateur comporte une section pour chaque niveau de la hiérarchie des applications. A chaque niveau du navigateur, les mesures du tableau de bord changent pour afficher les données du composant. Sélectionnez un élément pour basculer le contexte du tableau de bord vers la sélection. La portée de l'affichage est déterminée par vos droits utilisateur.

Chaque élément de navigateur possède un indicateur de statut critique, d'avertissement, normal ou inconnu, qui indique que l'agent n'est pas disponible. Chaque section de navigateur présente un certain nombre d'événements pour chaque gravité associée à l'élément de navigateur sélectionné. Pour en savoir plus sur le mappage des statuts aux événements de seuil, voir «Statut de l'événement», à la page 1156.

Pour libérer de l'espace pour d'autres sections, cliquez sur une barre de titre pour réduire la section et cliquez à nouveau dessus pour la restaurer. Vous pouvez également masquer entièrement le navigateur en cliquant sur  sur la bordure du navigateur, le restaurer en cliquant sur  , ou ajuster la largeur en faisant glisser la  bordure.

Le navigateur comporte trois sections :

- La section **Applications** répertorie toutes les applications définies de vos domaines ou disposant d'une autorisation pour votre rôle utilisateur.
  - Une fois que vous avez sélectionné une application, le tableau de bord affiche un récapitulatif général des statuts dans l'onglet **Présentation des statuts** et un indicateur du statut de gravité la plus élevée apparaît dans l'onglet **Evénements**. Pour plus d'informations, voir «Application - Tableau de bord d'Application Performance», à la page 1128.
  - Tous les composants de votre domaine qui ont été détectés par l'infrastructure de surveillance s'affichent dans l'application prédéfinie nommée «Mes composants», qui ne peut pas être modifiée ou supprimée.
  - Si vous disposez de droits administrateur, la barre d'outils Applications inclut des outils de gestion d'applications. Pour obtenir des instructions, voir «Gestion des applications», à la page 1145.
- Une fois que vous avez sélectionné une application, la section **Groupes** affiche les groupes prenant en charge l'application. Pour plus d'informations, voir «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1133.
- Une fois que vous avez sélectionné un sous-groupe, la section **Instances** est renommée pour le titre de sous-groupe et renseignée avec les noms des systèmes gérés individuels. L'onglet **Présentation des statuts** change et affiche les KPI du sous-groupe sélectionné. Après que vous sélectionnez un système géré, les widgets de groupe détaillés s'affiche avec les KPI du système géré. Pour les instances de composant, vous disposez également d'un onglet **Détails de l'attribut** qui affiche un tableau des indicateurs clés de performance des attributs de l'ensemble de données de votre choix. Pour plus d'informations, voir «Affichage et gestion de graphiques et tableaux personnalisés», à la page 1139.

Si un message popup **Erreur réseau** apparaît dans le navigateur, les indicateurs de statut peuvent passer à Normal jusqu'après la restauration de la connexion. A ce moment-là, tous les événements ouverts sont traités à nouveau et le statut affiché peut être Normal jusqu'à ce que le traitement soit terminé.

Recherche dans les fichiers journaux

Pour rechercher la cause première d'un problème rencontré par des utilisateurs, tel qu'une lenteur ou une défaillance, vous pouvez effectuer une recherche dans les données de journal associées à vos applications.

IBM Operations Analytics - Log Analysis fournit la fonction de recherche. Les données du journal d'application et les données de performances sont combinées pour vous aider à trouver la cause première d'un problème lié à vos applications et accélérer sa résolution.

Procédure

Effectuez les opérations suivantes pour chercher les entrées de journal qui peuvent être liées à un problème que vous examinez, par exemple, une utilisation élevée de l'unité centrale.

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**.
2. Si vous souhaitez effectuer une recherche dans une application, sélectionnez-la dans le tableau de bord «Toutes mes applications». Par exemple, cliquez sur «Mes composants» pour effectuer une recherche dans les journaux de toutes les ressources de composant.
3. Entrez le texte de fichier journal à rechercher dans la zone de recherche . Par exemple, entrez `annulé` pour rechercher les ressources Agent WebSphere Applications qui ont été restaurées au niveau précédent.
4. Si vous souhaitez rechercher des données dans une plage horaire autre que **Dernière heure**, cliquez sur et sélectionnez une période différente.
5. Cliquez sur .

Résultats

Toutes les entrées de journal contenant le texte à rechercher dans le contexte du niveau de navigateur en cours s'affichent dans un nouvel onglet ou une nouvelle fenêtre de navigateur. La fenêtre de navigateur est nommée en fonction du contexte, par exemple, application «de traitement des cartes de crédit».

Que faire ensuite

Examinez les résultats de la recherche. Vous pouvez sélectionner une autre application pour modifier les résultats de la recherche en fonction du contexte. Utilisez la zone de recherche pour affiner les résultats. Par exemple, si la zone de recherche montre `db2 AND (datasourceHostName:Pear* OR datasourceHostname:Persimmon* OR datasourceHostname:Pomegranate*)`, vous pouvez supprimer des sources de données pour limiter les résultats : `db2 AND (datasourceHostname:Persimmon*)`.

Pour plus d'informations, consultez l'ensemble de rubriques relatives à IBMOperations Analytics Log Analysis dans IBM Knowledge Center ou accédez à IBM Operations Analytics - Developers Community.

Application - Tableau de bord d'Application Performance

Après avoir sélectionné une application depuis le navigateur ou une zone récapitulative dans le tableau de bord **Toutes mes applications**, un tableau de bord à onglets présente les différentes facettes de votre application.

L'onglet **Présentation des statuts** présente un récapitulatif général du statut de votre application. Les indicateurs de seuil et de statut du graphique donnent des informations générales sur la santé et les performances. Sélectionnez l'onglet **Evénements** pour identifier les seuils d'événement qui contribuent à la santé de l'application.

Pour une description du navigateur et des éléments de bannière, voir «Navigateur», à la page 1126, «Rechercher», à la page 1126, «Actions», à la page 1126 et « Aide», à la page 1126.

présentation des statuts

- Selon la composition de l'application sélectionnée, l'onglet **Présentation des statuts** présente une ou plusieurs perspectives permettant d'évaluer le statut de l'application à un niveau global :

  Disponibilité dans le temps

  Le graphique à barres Disponibilité dans le temps s'affiche si l'application inclut l'Agent Synthetic Playback (dans le groupe de navigation Transactions et dans l'application prédéfinie, Mes transactions).

  Chaque point de tracé est un exemple de transaction comportant un indicateur de couleur pour un statut **Sain**, **Lent** ou **Non disponible**.

  Cliquez n'importe où sur la barre de temps pour ouvrir une fenêtre en incrustation avec les tables Liste des transactions et Liste des emplacements.

  Demandes et temps de réponse

  Le graphique à barres empilées Demandes et temps de réponse s'affiche si l'application inclut l'Agent de surveillance des temps de réponse (Transactions utilisateur final dans le groupe de navigation Transactions).

  Utilisez ce graphique pour examiner les motifs de tendance relatifs aux performances. Chaque barre empilée représente le pourcentage des demandes pour lesquelles le temps de réponse est correct, pour lesquelles le temps de réponse est lent, ou qui n'ont pas abouti. Le graphique à courbes représente le temps de réponse moyen au cours de la période de cinq minutes. Utilisez le sélecteur de durée pour modifier l'intervalle affiché, comme décrit dans «Ajustement et comparaison de mesures dans le temps», à la page 1138.

Agréger une topologie de transaction

Le widget Agréger une topologie de transaction s'affiche si le suivi des transactions est activé et que l'application sélectionnée comprend l'un des agents ou collecteurs de données suivants :

- agent DataPower
- agent HTTP Server
- agent IBM Integration Bus
- collecteur de données J2SE
- agent JBoss
- collecteur de données Liberty
- agent Microsoft .NET
- agent Microsoft SQL Server
- collecteur de données Node.js
- Agent de surveillance des temps de réponse
- Agent SAP NetWeaver Java Stack
- Agent Tomcat
- Agent WebLogic (Linux et Windows uniquement)
- Agent WebSphere Applications
- Agent WebSphere MQ

Vous devez activer manuellement le suivi des transactions pour tous les agents sauf pour l'Agent de surveillance des temps de réponse.Le suivi des transactions est activé automatiquement pour les collecteurs de données. Pour plus d'informations, voir «Page Configuration d'agent», à la page 218.

Le widget Agréger une topologie de transaction présente les ressources qui sont associées à l'application et leurs relations. Le pied de page indique le nombre des noeuds, ressources et relations sélectionnés, tous les filtres de la topologie ainsi que l'heure de la dernière régénération des données.

Si un composant d'application est ajouté à une application métier et que le composant transporte le trafic pour plusieurs applications, la topologie d'application qui s'affiche pour ces applications métier comprend les chemins vers les noeuds pour toutes les applications.

Dans le cadre de la Liste d'applications Java IBM, dans laquelle JavaScript est automatiquement injecté, le niveau de noeud le plus élevé représente le navigateur et le noeud le plus granulaire correspond à la base de données. Concernant les autres applications, le niveau de noeud le plus élevé représente l'application, alors que le noeud le plus granulaire correspond à l'instance du système géré.

Chaque noeud comporte un indicateur de statut et une mise en évidence d'arrière-plan qui montrent la gravité de statut la plus élevée à ce niveau d'agrégation. Si vous réduisez le navigateur afin de libérer de l'espace, vous pouvez continuer de voir le même statut dans le widget Agréger une topologie de transaction. L'environnement source du noeud s'affiche sous la forme **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **On Premises** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private) ou **Public Cloud** (IBM Cloud). Aucune icône n'est affichée pour **Autre** (la ressource gérée provient d'un autre environnement).

Faites passer la souris sur un noeud, ouvrez le menu de raccourci et sélectionnez des noeuds pour obtenir davantage d'informations sur le statut et ainsi identifier plus facilement la cause première d'un problème :

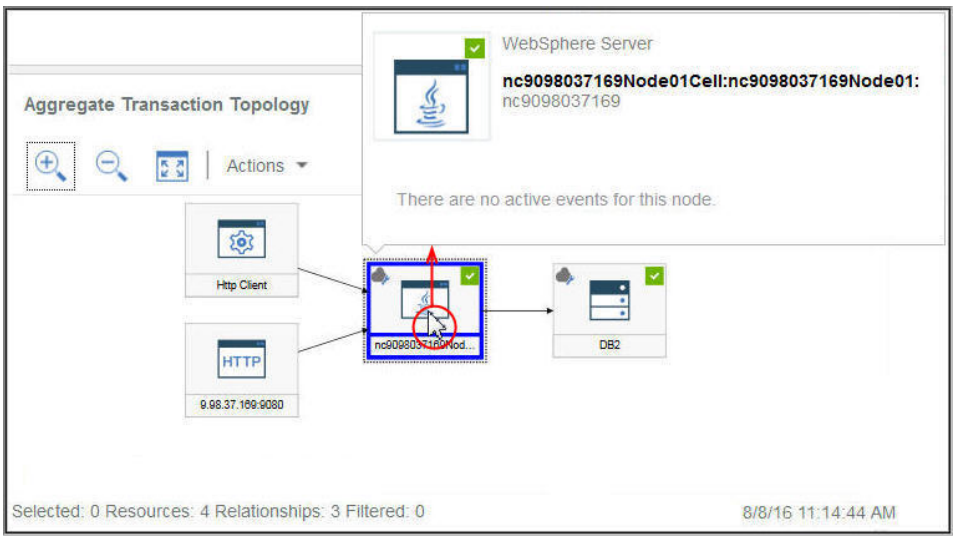
- Lorsque vous faites passer votre souris sur un noeud, un message en incrustation fournit une liste des événements critiques et d'avertissement.

– Cliquez deux fois sur une URL de lien dans un nœud afin d'ouvrir le tableau de bord correspondant qui présente les détails de composant ou de transaction.
– Cliquez avec le bouton droit de la souris sur un noeud et sélectionnez l'une des options d'analyse détaillée du tableau de bord : **Accéder à la page Récapitulatif des transactions** du noeud de sous-groupe sélectionné ; **Accéder à la page Instance de composant** du noeud d'instance ; ou **Propriétés** pour afficher le nom de la ressource, le statut, le nom du système géré et le domaine du fournisseur (tel que «Cloud»).

Utilisez les icônes de la barre d'outils pour ajuster l'affichage et suivez la procédure décrite dans «Manipulation du widget Agréger une topologie de transaction», à la page 1132.

Cliquez sur l'outil pour basculer entre cette vue et Statut courant des composants, décrit ci-après.

Les agents de surveillance sans information de topologie ne s'affichent pas dans le widget Agréger une topologie de transaction.



Statut courant des composants

Le graphique à barres empilées de statut de composant en cours indique le pourcentage et le nombre de statuts Critique, Avertissement, Normal et Inconnu pour chaque type de composant de l'application. Par exemple, cinq systèmes Linux prennent en charge l'application sélectionnée. Des barres empilées indiquant 40 % pour le statut Critique et 60 % pour le statut Normal signifient que deux systèmes ont le statut Critique et trois systèmes, le statut Normal.

Placez le pointeur de la souris sur une barre pour lire le statut dans une fenêtre en incrustation : le pourcentage et le nombre d'instances de composant possédant ce statut. Les domaines dans lesquels se trouvent les instances sont également affichés avec un statut pour chaque domaine : IBM Cloud, Cloud, On Premises, ITM et Autre. Par exemple, deux de vos cinq systèmes Linux se trouvent dans le domaine ITM et trois dans le domaine Cloud. Si l'un des systèmes critiques se trouve dans le domaine ITM et que l'autre se trouve dans le domaine Cloud, lorsque vous déplacez la souris sur le segment de la barre critique (40 %), la fenêtre en incrustation du statut affiche un système dans le domaine ITM et l'autre système dans le domaine Cloud.

Vous pouvez cliquer sur une barre pour ouvrir le tableau de bord récapitulatif de statut pour le type de composant, avec un widget de groupe pour chaque système surveillé.

Cliquez sur l'outil pour basculer entre cette vue et le widget Agréger une topologie de transaction décrite plus haut.

Transactions synthétiques

L'Agent Synthetic Playback a une application prédéfinie *Mes transactions* qui s'ouvre dans la page du tableau de bord du sous-groupe Transactions synthétiques. A partir de là, vous pouvez

descendre dans la hiérarchie jusqu'au niveau de l'instance de transaction. Pour plus d'informations, voir Surveillance de Synthetic Playback.

- Une fois que vous avez sélectionné un sous-groupe de la section **Groupes**, la section **Instances** est renommée pour le titre de sous-groupe et elle est renseignée avec les noms des instances individuelles. Pour plus d'informations sur les tableaux de bord au niveau du groupe, du sous-groupe et de l'instance du navigateur, ainsi que sur l'onglet **Détails d'attribut** qui s'affiche après la sélection d'un système géré, voir «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1133 et «Affichage et gestion de graphiques et tableaux personnalisés», à la page 1139.
- Certains widgets de tableau de bord montrent des mesures basées sur un intervalle, et d'autres montrent les mesures les plus récentes. Si une barre de sélection de durée s'affiche, vous pouvez ajuster l'intervalle pour le tableau de bord afin d'affecter tous les graphiques ou tableaux dont les valeurs sont dérivées de données historiques. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1138.
  Tout en visualisant les graphiques, vous pouvez cliquer sur un point de tracé pour ouvrir une infobulle indiquant la valeur du point de tracé et d'autres informations pertinentes. Lorsque vous avez fini d'afficher un graphique à courbes dans le navigateur Internet Explorer version 11, vous pouvez continuer de voir l'infobulle pendant que vous déplacez le curseur autour de la fenêtre. Si vous rencontrez ce comportement, vous pouvez fermer l'infobulle en cliquant plusieurs fois dans le graphique.
- Les données sont actualisées automatiquement toutes les minutes dans la console. Cette activité est essentielle et ne peut pas être interrompue, arrêtée ni masquée.
- Si aucune donnée n'est disponible pour un graphique ou une zone récapitulative de statut, un message d'information s'affiche.

Evénements

- Les indicateurs de statut qui s'affichent en regard du titre d'onglet **Evénements**, tels que **14** **3**, indiquent le nombre de gravités d'événement les plus élevées pour l'élément de navigateur sélectionné : application, groupe, sous-groupe ou instance. Les gravités des seuils sont consolidées, comme illustré dans le tableau suivant. Par exemple, **Evénements** signifie que l'événement ayant la gravité maximale est mineur ou correspond à un avertissement.

Onglet Evénements	Gravité de seuil
Critique	Fatal et Critique
Avertissement	Mineur et Avertissement
Normal	Inconnu

  Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights et qu'une anomalie est détectée, un événement est ouvert. Une icône en forme de diamant recouvre l'indicateur de statut, par exemple, , pour vous informer qu'au moins une anomalie a été détectée par Operations Analytics - Predictive Insights. Par exemple, **Evénements** , indique que l'événement de statut le plus élevé est Avertissement, et qu'au moins un événement d'anomalie est ouvert.
- Cliquez sur l'onglet **Evénements** pour afficher le récapitulatif du nombre total d'événements, le nombre d'événements pour chaque type de gravité et une jauge en pourcentage des gravités. Pour plus d'informations, voir «Statut de l'événement», à la page 1156.

Vues personnalisées

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Par exemple, l'application Inventory Management dans Cloud APM Démonstration guidée possède les agents de surveillance suivants : Linux OS, MySQL, Node.js, Hadoop et Ruby. Vous pouvez créer et sauvegarder une page personnalisée à n'importe quel niveau du navigateur allant de l'application à l'instance, puis l'ouvrir au niveau où elle a été créée. Une page créée à un niveau particulier ne peut être ouverte qu'au même niveau. Les mesures disponibles pour les widgets peuvent être des ressources, quelles qu'elles

soient, de l'application. A l'aide de l'exemple Inventory Management, vous pouvez créer une page avec une table à partir de l'Agent Ruby, un graphique à partir de l'Agent Linux OS, etc.

- L'onglet **Vues personnalisées** est disponible à n'importe quel niveau du navigateur lorsque vous sélectionnez une application dans Toutes mes applications.
- Une fois que vous avez ouvert l'onglet **Vues personnalisées**, la fenêtre de sélection d'un modèle pour votre page personnalisée est affichée ou la page par défaut est affichée si elle est déjà définie.
  - Dans la fenêtre de sélection d'un modèle pour votre page personnalisée, vous pouvez sélectionner un modèle pour créer une page.
  - Dans la page par défaut, vous pouvez cliquer sur  pour créer une page.
- Dans la page par défaut, cliquez sur dans la liste des pages et sélectionnez l'une des pages sauvegardées de la liste.
- Les options disponibles dans l'onglet Vues personnalisées varient selon que la page soit éditée ou consultée. Pour plus d'informations sur l'édition d'une page, voir «Création et gestion de pages personnalisées», à la page 1160. Pour plus d'informations sur l'affichage d'une page, voir «Affichage de pages personnalisées», à la page 1167.

Manipulation du widget Agréger une topologie de transaction

Utilisez le widget Agréger une topologie de transaction pour afficher la hiérarchie des ressources dans l'application sélectionnée. Vous pouvez ajuster et déplacer l'affichage pour voir le statut de chaque composant et sa relation avec les autres composants, et ouvrir le tableau de bord correspondant.

Avant de commencer

Une fois que vous avez sélectionné une application dans le Tableau de bord d'Application Performance, l'onglet **Présentation des statuts** s'affiche avec un ou plusieurs graphiques, en fonction des ressources surveillées incluses dans l'application.

Le widget Agréger une topologie de transaction s'affiche pour les agents suivants qui prennent en charge le suivi des transactions :

- agent DataPower
- agent HTTP Server
- agent IBM Integration Bus
- collecteur de données J2SE
- agent JBoss
- collecteur de données Liberty
- agent Microsoft .NET
- agent Microsoft SQL Server
- collecteur de données Node.js
- Agent de surveillance des temps de réponse
- Agent SAP NetWeaver Java Stack
- Agent Tomcat
- Agent WebLogic (Linux et Windows uniquement)
- Agent WebSphere Applications
- Agent WebSphere MQ

Agréger une topologie de transaction affiche un objet de noeud pour chaque ressource surveillée qui prend en charge la fonction de topologie.

Procédure

Effectuez l'une des étapes suivantes pour manipuler le widget Agréger une topologie de transaction et ouvrir des tableaux de bord qui sont associés aux noeuds :

- Pour ouvrir un tableau de bord lié, cliquez deux fois sur le noeud de topologie. Vous pouvez également cliquer avec le bouton droit de la souris sur un noeud et sélectionner l'une des options d'analyse détaillée du tableau de bord, **accéder à la page Récapitulatif des transactions**, **accéder à la page Instance de composant** ou sélectionner **Propriétés** pour afficher les informations relatives au système géré.
- Pour agrandir la taille d'affichage de la topologie, cliquez sur **Zoom avant**. Vous pouvez également cliquer sur **Actions** > **Zoom avant** si aucun noeud n'est sélectionné.
- Pour réduire la taille d'affichage de la topologie, cliquez sur **Zoom arrière**. Vous pouvez également cliquer sur **Actions** > **Zoom arrière** si aucun noeud n'est sélectionné.
- Pour ajuster la taille d'affichage de la topologie afin de l'adapter à l'espace de widget en cours, cliquez sur **Ajuster au contenu**. Vous pouvez également cliquer sur **Actions** > **Ajuster au contenu** si aucun noeud n'est sélectionné.
- Pour filtrer les noeuds de la topologie, sélectionnez l'un des indicateurs dans la barre de filtre. Vous pouvez activer et désactiver les filtres et sélectionner plusieurs filtres. Tous les noeuds comportant une propriété ne correspondant pas au filtre apparaissent en grisé, tandis que ceux correspondant au filtre restent visibles.
  - Normal, Avertissement, Critique ou Inconnu pour filtrer par statut de noeud.
  - Pour filtrer par environnement, sélectionnez **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **On Premises** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private) ou **Public Cloud** (IBM Cloud).
  - Filtrer pour ajouter un filtre personnalisé.
- Pour libérer de l'espace pour le widget de topologie, cliquez sur la **section de réduction** du navigateur ou sur les widgets de graphique environnants ou faites glisser une bordure de widget .

Groupe et Instance - Tableau de bord d'Application Performance

Utilisez le tableau de bord du groupe, du sous-groupe ou de l'instance de l'application sélectionnée pour obtenir un statut de haut niveau de vos systèmes gérés. Vous pouvez accéder jusqu'au niveau des tableaux de bord détaillés comportant des mesures associées à l'instance sélectionnée et créer des graphiques et des tableaux personnalisés.

Une fois que vous avez sélectionné une application sous **Toutes mes applications** dans le Tableau de bord d'Application Performance, les onglets Présentation des statuts et Evénements s'affichent.

La section **Groupes** du navigateur affiche un ou plusieurs groupes possibles, selon les éléments de l'application définie.

Pour une description du navigateur et des éléments de bannière, voir «Navigateur», à la page 1126, «Rechercher», à la page 1126, «Actions», à la page 1126 et « Aide», à la page 1126.

présentation des statuts

Groupes et sous-groupes

- Sélectionnez un groupe ou développez un groupe et sélectionnez un sous-groupe pour voir un widget de groupe récapitulatif pour chaque système géré dans l'application. Lorsqu'un sous-groupe est sélectionné, les widgets de groupe récapitulatif dans l'onglet Présentation des statuts sont propres à ce sous-groupe.

- Les groupes prédéfinis disponibles sont les suivants, selon les produits de surveillance installés :

  Composants
  Ce groupe s'affiche pour toutes les applications, à l'exception de l'Agent de surveillance des temps de réponse, de l'Agent Synthetic Playback et d'Availability Monitoring.

  Le groupe Composants comporte un sous-groupe pour chaque composant logiciel surveillé qui prend en charge l'application sélectionnée.

  Transactions
  Ce groupe inclut Transactions utilisateur finalet Transactions synthétiques . Pour plus d'informations, voir l'aide de la surveillance des transactions et de l'Agent Synthetic Playback ou leurs PDF de référence sur l'APM Developer Center sous Agent metrics/Reference PDFs.

- Une fois que vous avez sélectionné **Composants** ou un sous-groupe de la section **Groupes**, l'onglet Présentation des statuts change et affiche un tableau de bord récapitulatif avec un widget de groupe pour chaque ressource gérée. L'environnement source s'affiche sous forme de **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **On Premises** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private) ou **Public Cloud** (IBM Cloud). La section Instances est renommée pour le titre de sous-groupe et elle est renseignée avec les noms des différentes instances.



  Si l'application compte de nombreuses instances de système géré, de nombreux widgets de groupe sont affichés. Vous pouvez parcourir la liste pour les afficher tous. Vous pouvez également sélectionner un type de système géré de la liste de sous-groupes de composants, tels que le système d'exploitation Windows, pour confiner l'affichage aux mêmes types de système géré. Vous pouvez également filtrer les instances de système géré.

  Navigateur Firefox seulement : selon le nombre d'agents et la bande passante, à mesure que vous descendez dans la page Composants, un message en incrustation vous avertira sans doute que le script de chargement de la page de ressource prend un certain temps pour se terminer. Sélectionnez l'option «Don't ask me again» pour désactiver le message et continuer à ouvrir les widgets. Vous pouvez également entrer `about:config` dans la zone d'adresse, rechercher **`dom.max_script_run_time`** et accroître la valeur de délai (en secondes). La valeur zéro (0) désactive le délai d'attente.

Instances

- Cliquez dans un widget de groupe ou sélectionnez le nom de l'instance dans le navigateur afin d'ouvrir un tableau de bord détaillé de la ressource gérée.
- Si plusieurs instances s'affichent dans le navigateur, utilisez la zone de recherche dans la barre d'outils Instances. A mesure de la frappe dans cette zone, toute instance qui ne concorde pas est supprimée de l'affichage.

- Pour mettre en pause l'actualisation automatique du Tableau de bord d'Application Performance, cliquez sur Pause dans la barre d'outils Instances ; pour reprendre l'actualisation automatique, cliquez sur Reprise.
- Les widgets et indicateurs clés de performance qui s'affichent pour un système géré peuvent dépendre de la version de l'agent. Si un agent est installé sur le système géré à un niveau de version antérieur, il se peut qu'il ne puisse pas fournir autant d'informations que la version actuelle de l'agent. Un message s'affiche à la place d'un ou plusieurs indicateurs clés de performance dans un graphique ou un tableau lorsqu'aucune donnée n'est disponible. Cela peut simplement être dû au fait qu'aucune donnée n'a été signalée pour l'intervalle de temps. Sinon, cette situation peut être liée au fait qu'un agent de niveau antérieur qui ne prend pas en charge l'ensemble de données ou un attribut est inclus dans le graphique ou le tableau.
  Pour obtenir la liste des tableaux de bord d'agent mis à jour depuis le dernier redémarrage du serveur Cloud APM, sélectionnez **Actions** > **Journal de tableau de bord**.
- Certains widgets de tableau de bord montrent des mesures basées sur un intervalle, et d'autres montrent les mesures les plus récentes. Si une barre de sélection de durée s'affiche, vous pouvez ajuster l'intervalle pour le tableau de bord afin d'affecter tous les graphiques ou tableaux dont les valeurs sont dérivées de données historiques. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1138.
  Tout en visualisant les graphiques, vous pouvez cliquer sur un point de tracé pour ouvrir une infobulle indiquant la valeur du point de tracé et d'autres informations pertinentes. Lorsque vous avez fini d'afficher un graphique à courbes dans le navigateur Internet Explorer version 11, vous pouvez continuer de voir l'infobulle pendant que vous déplacez le curseur autour de la fenêtre. Si vous rencontrez ce comportement, vous pouvez fermer l'infobulle en cliquant plusieurs fois dans le graphique.
- Si vous consultez un graphique dont certaines barres sont manquantes, cela signifie que la valeur de ce point de données correspond à 0 (zéro).



- Les utilisateurs d'IBM Cloud Application Performance Management, Advanced Private disposent de tableaux de bord de diagnostic supplémentaires auxquels vous pouvez accéder en cliquant sur le lien **Diagnostiquer** à partir d'un widget de groupe dans le tableau de bord Détails.

  Restriction : Le système géré pour lequel vous ouvrez les tableaux de bord de diagnostic doit résider dans le domaine IBM Cloud APM. Si le système géré réside dans le domaine source IBM Cloud ou IBM Tivoli Monitoring, les tableaux de bord de diagnostic ne sont pas disponibles. Voir aussi «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 872.
- Si votre environnement inclut l'Agent Synthetic Playback, vous pouvez lancer les rapports Cloud APM pour l'instance d'agent à partir du menu **Actions**.

Evénements

- Les indicateurs de statut qui s'affichent en regard du titre d'onglet **Evénements**, tels que **14** **3**, indiquent le nombre de gravités d'événement les plus élevées pour l'élément de navigateur sélectionné : application, groupe, sous-groupe ou instance. Les gravités des seuils sont consolidées, comme illustré dans le tableau suivant. Par exemple, **Evénements** signifie que l'événement ayant la gravité maximale est mineur ou correspond à un avertissement.

Onglet Evénements	Gravité de seuil
Critique	Fatal et Critique
Avertissement	Mineur et Avertissement
Normal	Inconnu

Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights et qu'une anomalie est détectée, un événement est ouvert. Une icône en forme de diamant recouvre l'indicateur de statut, par exemple, , pour vous informer qu'au moins une anomalie a été détectée par Operations Analytics - Predictive Insights. Par exemple, **Evénements** , indique que l'événement de statut le plus élevé est Avertissement, et qu'au moins un événement d'anomalie est ouvert.

- Cliquez sur l'onglet **Evénements** pour afficher le récapitulatif du nombre total d'événements, le nombre d'événements pour chaque type de gravité et une jauge en pourcentage des gravités. Pour plus d'informations, voir «Statut de l'événement», à la page 1156.

Vues personnalisées

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Par exemple, l'application Inventory Management dans Cloud APM Démonstration guidée possède les agents de surveillance suivants : Linux OS, MySQL, Node.js, Hadoop et Ruby. Vous pouvez créer et sauvegarder une page personnalisée à n'importe quel niveau du navigateur allant de l'application à l'instance, puis l'ouvrir au niveau où elle a été créée. Une page créée à un niveau particulier ne peut être ouverte qu'au même niveau. Les mesures disponibles pour les widgets peuvent être des ressources, quelles qu'elles soient, de l'application. A l'aide de l'exemple Inventory Management, vous pouvez créer une page avec une table à partir de l'Agent Ruby, un graphique à partir de l'Agent Linux OS, etc.

- L'onglet **Vues personnalisées** est disponible à n'importe quel niveau du navigateur lorsque vous sélectionnez une application dans Toutes mes applications.
- Une fois que vous avez ouvert l'onglet **Vues personnalisées**, la fenêtre de sélection d'un modèle pour votre page personnalisée est affichée ou la page par défaut est affichée si elle est déjà définie.
  - Dans la fenêtre de sélection d'un modèle pour votre page personnalisée, vous pouvez sélectionner un modèle pour créer une page.
  - Dans la page par défaut, vous pouvez cliquer sur pour créer une page.
- Dans la page par défaut, cliquez sur dans la liste des pages et sélectionnez l'une des pages sauvegardées de la liste.
- Les options disponibles dans l'onglet Vues personnalisées varient selon que la page soit éditée ou consultée. Pour plus d'informations sur l'édition d'une page, voir «Création et gestion de pages personnalisées», à la page 1160. Pour plus d'informations sur l'affichage d'une page, voir «Affichage de pages personnalisées», à la page 1167.

Détails d'attribut

- L'onglet **Détails d'attribut** s'affiche après que vous avez sélectionné une instance de composant dans la section Instances du navigateur (renommée avec le nom du sous-groupe sélectionné) ou si vous cliquez dans un widget de groupe récapitulatif.
- Si des pages de graphique ou de tableau ont été sauvegardées pour l'agent, la page récemment ouverte est affichée avec des valeurs de l'instance de composant sélectionnée. Cliquez sur le titre pour sélectionner une autre page à partir de **Mes pages** ou **Pages partagées** .
- Vous pouvez modifier le graphique ou le tableau et cliquer sur **Prévisualiser les résultats** pour afficher le graphique ou le tableau avec les attributs sélectionnés. Pour plus d'options, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1140.

Edition des widgets de groupe du tableau de bord Composants

Vous pouvez éditer les valeurs de seuil des widgets de groupe qui s'affichent dans le tableau de bord Composants (sélectionné dans la section Groupes du navigateur). Vous pouvez également contrôler l'affichage et la position des widgets de groupe, et décider s'il convient d'inclure un seuil de widget dans la détermination du statut de composant.

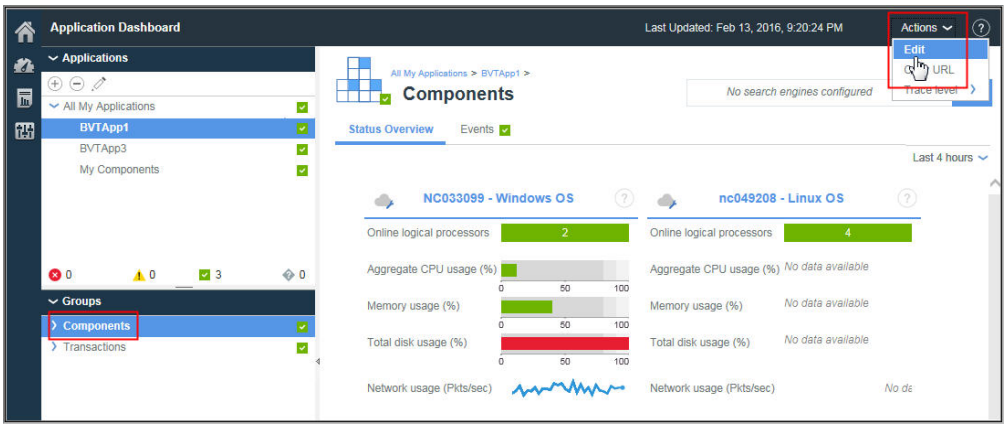
Pourquoi et quand exécuter cette tâche

Cette tâche implique l'édition du tableau de bord du groupe Composants et de son widget de groupe récapitulatif pour une application définie. L'éditeur du groupe Composants n'est pas disponible pour l'application prédéfinie Mes composants. Pour plus d'informations sur les applications définies, voir «Gestion des applications», à la page 1145.

Votre ID utilisateur doit également disposer de l'autorisation de modification du Tableau de bord d'Application Performance et de l'autorisation de création d'applications. Pour plus d'informations, voir «Rôles et droits», à la page 1021.

Procédure

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, sélectionnez l'application dont vous souhaitez éditer les widgets de groupe récapitulatif dans le tableau de bord Toutes mes applications.
2. Dans la section Groupes du navigateur, cliquez sur **Composants** afin d'ouvrir un tableau de bord présentant les widgets de groupe pour tous les composants de l'application.
3. Cliquez sur **Actions** > **Editer** pour ouvrir l'éditeur des widgets de groupe dans le groupe Composants. L'option **Editer** ne s'affiche que lorsque le tableau de bord Composants est ouvert.



4. Apportez l'une des modifications suivantes aux widgets de groupe :
   - Pour supprimer un widget de groupe de la vue, cliquez sur .
   - Pour modifier les seuils récapitulatifs d'un widget, cliquez sur Paramètres, sélectionnez l'onglet Seuils et modifiez les valeurs du niveau de gravité critique, avertissement ou normale. Après avoir modifié les seuils pour le widget de groupe, cliquez sur **Terminé**.
   - Pour ajouter un widget, cliquez sur , cliquez sur les icônes des applications jusqu'à ce que celle de votre choix s'affiche, cliquez dans le widget de groupe pour le sélectionner, puis cliquez sur **Ajouter**.
   - Pour redimensionner un widget, faites glisser l'icône de poignée . Le redimensionnement d'un widget ne modifie pas la taille du texte qu'il contient, ni sa hauteur.
   - Pour déplacer un widget, faites-le glisser vers sa nouvelle position.
5. Pour sauvegarder vos modifications et fermer l'éditeur, cliquez sur **Sauvegarder**, ou cliquez sur **Annuler** pour supprimer vos modifications.

Résultats

Le tableau de bord Composants de l'application sélectionnée s'affiche avec les nouveaux paramètres.

Que faire ensuite

Pour plus d'informations sur le tableau de bord lorsqu'un groupe ou sous-groupe est sélectionné dans le navigateur, voir «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1133 ; pour plus d'informations sur le tableau de bord de composant surveillé, cliquez sur le bouton dans la bannière Tableau de bord des applications.

Ajustement et comparaison de mesures dans le temps

Certains graphiques de tableau de bord montrent des mesures basées sur un intervalle et d'autres montrent uniquement les mesures les plus récentes.

Si une barre de sélection de durée est affichée dans l'onglet Présentation des statuts d'une instance de système géré, vous pouvez ajuster la période des graphiques dont les valeurs sont dérivées des échantillons de données historiques. Pour les attributs dont les données ont été collectées pour plusieurs jours et présentées dans un graphique à courbes, vous pouvez comparer les valeurs du jour à celles d'un jour précédent.

Avant de commencer

Si vous effectuez une comparaison avec un intervalle horaire d'un jour précédent, la date jusqu'à laquelle vous pouvez remonter dépend du nombre de jours que le serveur Cloud APM a enregistrés et du type des données affichées dans la page. Pour la plupart des jeux de données de surveillance, les échantillons de données sont stockés pendant une période de 8 jours. Le nombre exact est publié dans l'aide sur les attributs de l'agent ou du collecteur de données, ainsi que dans le PDF de référence (voir Chapitre 2, «Documentation au format PDF», à la page 29). Les données de suivi des transactions de l'Agent de surveillance des temps de réponse ou des agents middleware concernent uniquement les dernières 24 heures (ou dans certains cas les 4 dernières heures) et leur durée de conservation ne peut pas être modifiée.

Vous pouvez configurer votre serveur Cloud APM de sorte qu'il stocke jusqu'à 32 jours de données de surveillance des ressources pour les agents et collecteurs de données IBM sélectionnés. Pour plus d'informations, voir Gestion des valeurs de conservation des données d'historique.

Procédure

Pour ajuster l'intervalle horaire affiché dans le graphique à courbes pour une instance de ressource gérée ou comparer les valeurs au même intervalle horaire d'un jour précédent, procédez comme suit :

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**.
2. Accédez à la page de tableau de bord d'une instance qui présente les graphiques à courbes historiques et cliquez sur le sélecteur de durée **4 dernières heures**.
3. Sélectionnez une ou plusieurs des options suivantes :
   - Pour modifier l'intervalle affiché, sélectionnez **4 dernières heures**, **12 dernières heures** ou **Dernier jour**.
   - Pour comparer l'intervalle affiché dans un graphique à courbes avec les mesures d'un autre jour, sélectionnez **Comparer à** et sélectionnez un jour antérieur, jusqu' au nombre de jours indiqués comme disponibles dans le calendrier en incrustation (les dates non disponibles sont barrées).
   - Pour que l'intervalle s'applique à tous les tableaux de bord de toutes les applications définies dans votre environnement surveillé, sélectionnez **Toutes les applications**. Sinon, laissez le paramètre

défini sur **Uniquement cette application** pour appliquer l'intervalle uniquement à l'application en cours (par exemple «Mes composants»). La sélection **Comparer à** n'est effective que pour la page en cours.

Résultats

- Si vous visualisez des données historiques sans comparaison, tous les tableaux de bord de l'application en cours (ou de toutes les applications) sont affectés par la modification.
- Si vous visualisez une comparaison, seuls les graphiques à courbes de la page en cours sont affectés. Une ligne est tracée pour chaque indicateur clé de performance afin de présenter les mesures du jour choisi. Certains graphiques à courbes sont indisponibles pour la comparaison, comme indiqué par une cote d'alerte sur le graphique : «Aucune comparaison disponible». Cela peut se produire avec les ressources gérées les plus récentes n'ayant pas encore collectées de données pour la date spécifiée. Essayez de sélectionner une date plus récente pour la comparaison.
- Les widgets pour lesquels les données d'historique ne sont pas collectées continuent d'afficher les valeurs les plus récentes.
- Les points de données sont répartis sur toute la longueur du graphique pour l'intervalle sélectionné. Les horodatages sont affichés sur l'étiquette d'axe, des plus anciens aux plus récents. Vérifiez l'échantillon de données le plus ancien pour confirmer si les données d'historique sont affichées partiellement ou en totalité.
- Les données envoyées aux graphiques et aux tableaux sont normalisées au temps moyen de Greenwich. L'axe **Horodatage** imprime les horodatages en fonction du fuseau horaire de votre navigateur. Si votre horodatage utilise l'heure d'été, l'horodatage affiché pendant l'heure de transition est décalé d'une heure. Imaginez par exemple que vous affichez un graphique à courbes en Espagne et qu'à 2h00, il est désormais 3h00 suite au passage à l'heure d'été. En raison de la différence entre l'heure des données au temps moyen de Greenwich et l'heure locale de l'horodatage, celui-ci comporte un écart d'une heure entre 2h00 et 3h00. Si vous affichez le même graphique en Nouvelle-Zélande lors du passage de l'heure d'été (3h00) à l'heure d'hiver (2h00), les horodatages de 2h00 à 3h00 sont répétés.

Affichage et gestion de graphiques et tableaux personnalisés

Le Tableau de bord d'Application Performance fournit des tableaux de bord prédéfinis des indicateurs clés de performance de votre système géré. Lorsque vous visualisez le tableau de bord d'une instance de composant, utilisez l'onglet **Détails d'attribut** pour afficher des pages de graphiques ou de tableaux sauvegardées et créer et gérer d'autres pages.

Par exemple, vous observez un indicateur critique dans le tableau de bord récapitulatif. Vous accédez alors au niveau de l'instance dans laquelle cette condition a été constatée. A cet emplacement, vous ajoutez un graphique illustrant le débit de l'unité centrale occupée pour observer les événements sur une période donnée. Vous pouvez afficher des détails sur tout attribut disponible de l'instance de composant sélectionnée et sauvegarder le graphique ou le tableau personnalisé avec l'agent et l'afficher chaque fois que vous ouvrez une instance de système géré.

Un sous-ensemble des attributs et des ensembles de données de l'agent est disponible pour l'utilisation dans les tables et les graphiques personnalisés. Ces attributs sont les plus utiles pour l'affichage dans les tableaux de bord. L'ensemble complet des attributs peut être utilisé dans les seuils personnalisés (voir «Gestionnaire de seuils», à la page 1002).

Pour améliorer les performances et réduire la redondance, les agents restreignent le nombre de lignes affichées pour certains ensembles de données dans les détails d'attribut. Les descriptions des ensembles de données dans l'aide et le fichier PDF de l'agent indiquent si l'échantillon de données par défaut limite le nombre de lignes envoyées au serveur Cloud APM.

Pour les utilisateurs malvoyants, la possibilité de créer des tables historiques fournit une alternative aux graphiques à courbes que les technologies d'assistance aux personnes handicapées, telles les logiciels de lecteur d'écran, ne peuvent pas interpréter. L'onglet **Détails d'attribut**, disponible pour les instances de

transaction de l'Agent de surveillance des temps de réponse et de l'Agent Synthetic Playback, vous permet ainsi de créer des tables historiques. Pour plus d'informations, voir «Exemple de création d'une table personnalisée avec les commandes du clavier», à la page 1143.

Création d'une page de graphiques ou de tableaux personnalisés

Lorsque vous visualisez le Tableau de bord d'Application Performance d'une instance de composant, vous pouvez sélectionner l'onglet **Détails d'attribut** pour afficher des pages de graphiques ou de tableaux sauvegardées, ainsi que pour créer et gérer d'autres pages.

Pourquoi et quand exécuter cette tâche

Lorsque vous êtes dans la page d'accueil du Tableau de bord d'Application Performance et que vous descendez dans la hiérarchie jusqu'à une instance de votre ressource gérée, l'onglet **Détails d'attribut** est ajouté aux onglets **Présentation des statuts** et **Evénements** sur la page du tableau de bord.

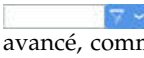
Ces instructions concernent la création de graphiques et de tableaux personnalisés pour les instances de composant. Vous pouvez suivre les étapes relatives aux instances de transaction de l'Agent de surveillance des temps de réponse et de l'Agent Synthetic Playback, avec les limitations suivantes : tables historiques uniquement (pas de graphiques) ; impossibilité de filtrer la liste des **fichiers** ou des **attributs** ; sélection de tous les attributs (vous ne pouvez ni sélectionner, ni désélectionner des attributs individuels) ; impossibilité de sauvegarder la page ; indisponibilité de l'option **Précédent** dans le sélecteur de temps pour l'Agent Synthetic Playback.

Procédure

Pour créer un graphique ou un tableau à partir d'un fichier disponible pour l'instance de composant surveillée, procédez comme suit :

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, accédez au niveau d'une instance de la ressource gérée. Le système sélectionné est mis en évidence dans la section Instances du navigateur, avec un nom basé sur le type de composant, par exemple Ruby App.
2. Cliquez sur l'onglet **Détails d'attribut**. Si aucune page de graphiques ou de tableaux n'a été enregistrée pour ce type d'agent de surveillance, **Temps réel** **Tableau** est sélectionné. Temps réel est approprié pour les ensembles de données qui renvoient plusieurs lignes et n'est disponible que pour les tableaux.
3. Si une page de graphiques ou de tableaux est affichée, cliquez sur **Nouveau**.
4. Entrez un nom pour la page de graphiques ou de tableaux dans la zone de titre. N'utilisez aucun des caractères suivants dans le titre : `! " % & ' * ? < > } { \`.
5. Si vous préférez afficher des échantillons de données au fil du temps, modifiez le type pour **Historique**. L'option **Graphique** est activée.
6. Si vous avez sélectionné **Historique** et que vous préférez obtenir un graphique plutôt qu'un tableau, cliquez sur **Graphique**.
7. Depuis la liste **Ensemble de données**, sélectionnez le bouton d'option du type d'attributs que vous voulez afficher. Si la liste est longue, utilisez la zone de filtre pour réduire la liste en entrant le texte qui doit figurer dans l'ensemble de données. Par exemple, l'attribut «config» pour l'agent de système d'exploitation Linux, filtre les ensembles de données pour n'afficher que les ensembles de données Linux_CPU_Config et Linux_OS_Config.
8. Pour inclure un attribut dans le graphique ou le tableau, sélectionnez la case à cocher à côté du nom concerné dans la liste **Attributs** ou sélectionnez la case à cocher située en début de liste pour sélectionner tous les attributs. Entrez le texte dans la zone de filtre pour localiser des attributs spécifiques comme «percent». Par exemple, l'attribut «percent» dans l'ensemble de données KLZ_VM_Stats, filtre la liste pour n'afficher que l'attribut Espace de stockage virtuel disponible (pourcentage) et 5 autres attributs «Pourcentage». Les graphiques peuvent tracer uniquement des valeurs numériques. Tous les attributs de texte ou de date/heure sont désactivés.

9. Cliquez sur **Prévisualiser les résultats** pour générer la page avec les ensembles de données choisis, un regroupement par colonne de tableau ou ligne du graphique pour chaque attribut, et une ligne ou un point pour chaque échantillon de données. Vous obtenez également une ligne ou une ligne de tracé pour l'agrégat de toutes les valeurs.
10. Pour masquer des lignes de graphique ou de tableau, effectuez l'une des étapes suivantes :

Option	Description
Graphique	Masquez une mesure (une ligne du graphique) en désélectionnant la case située en regard du nom dans la légende. Cochez une case pour afficher une mesure.
Tableau	Réduisez le nombre de lignes affichées en entrant la valeur à utiliser pour le filtrage dans la zone de filtre  . Vous pouvez également créer un filtre avancé, comme décrit dans «Définition d'un filtre de tableau», à la page 1144.

11. Pour modifier l'intervalle, utilisez le sélecteur de temps :

Option	Description
Temps réel	Pour les tableaux seulement, actualise et affiche uniquement les derniers échantillonnages de données.
2 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des deux dernières heures, à intervalles réguliers.
4 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des quatre dernières heures, à intervalles réguliers.
12 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des douze dernières heures, à intervalles réguliers.
24 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des dernières vingt-quatre heures, à intervalles réguliers.
Précédent	Sous-menu d'options permettant d'inclure des données depuis la même période **Hier**, **Il y a deux jours** ou depuis n'importe quel jour jusqu'à **Il y a une semaine**. Par exemple, nous sommes le 22 août à 14h10 et vous définissez le graphique ou le tableau de sorte qu'il affiche les 4 dernières heures. Si vous sélectionnez **Précédent** > **Il y a 1 semaine**, vous voyez des points de données allant de 10h10 à 14h10, au jour d'aujourd'hui, et de 10h10 à 14h10 le 15 août. Si vous sélectionnez un jour précédent, le sélecteur de temps affiche un astérisque (*) tel que  et les données du jour sélectionné sont réactualisées :

- Vous pouvez uniquement visualiser les données dont la date est comprise entre la date du jour et une semaine auparavant (même si vous avez redéfini la durée maximale de conservation des données historiques sur une valeur supérieure à 8 jours).
- Les graphiques historiques sont représentés de l'échantillon de données le plus ancien au plus récent pour l'intervalle sélectionné ; par exemple, ces 4 dernières heures. Lorsqu'un jour précédent est sélectionné, vous visualisez les données dont la date est comprise entre l'intervalle sélectionné la veille et l'intervalle du jour. Tous les jours compris entre la date la plus ancienne et aujourd'hui montrent un point de tracé avec un horodatage et sans échantillon de données.

- Les tables historiques sont représentées dans l'ordre chronologique décroissant. Lorsqu'un jour précédent est sélectionné pour l'Agent de surveillance des temps de réponse, chaque colonne est répliquée pour le jour précédent avec la mention«Précédent» dans l'en-tête de colonne.
- Quel que soit l'intervalle sélectionné, 11 000 lignes au maximum peuvent être affichées. Par exemple, si vous choisissez d'afficher 12 heures d'un ensemble de données qui envoie 7000 lignes en 2 heures, moins de 3 heures de données d'historique sont renvoyées et les échantillons de données les plus anciens s'affichent.

12. Pour sauvegarder ou apporter des modifications au graphique ou au tableau, sélectionnez l'une des options suivantes :

Option	Description
Editer	Renvoie à l'éditeur pour apporter les modifications suivantes : • Editer le titre • Accéder aux échantillons de données **Temps réel** ou **Historique** • Accéder à **Graphique** ou **Tableau** • Sélectionner un **Ensemble de données** et/ou des **Attributs** différents.
Nouveau	Annule toutes les modifications non sauvegardées apportées à la vue en cours et vous renvoie à la page de sélection pour créer un nouveau graphique ou tableau.
Annuler	Annule la session d'édition pour la page de graphiques ou de tableaux en cours.
Supprimer	Supprime la page. **Supprimer** est uniquement disponible lorsqu'une page est enregistrée et qu'une édition en cours est annulée.
Sauvegarder pour moi	Enregistre la page de graphiques ou de tableaux pour l'affichage par votre ID utilisateur uniquement. Aucun autre utilisateur ne peut afficher la page enregistrée.
Sauvegarder pour partager	Enregistre la page de graphiques ou de tableaux pour l'affichage par n'importe quel ID utilisateur connecté à la console Cloud APM.

Les vues que vous sauvegardez ont un verrou ouvert à côté du titre. Les vues qu'un autre utilisateur a sauvegardées et que vous n'avez pas le droit d'éditer ont une icône de verrou fermé.

Résultats

Une fois le graphique ou le tableau personnalisé enregistré, il est ajouté à la liste des pages sauvegardées. Lorsque vous sélectionnez à nouveau une instance du même type de source de données, par exemple WebSphere Applications, et que vous sélectionnez l'onglet **Détails d'attribut**, la page enregistrée récemment ouverte est affichée. Cliquez sur le titre pour sélectionner une autre page à partir de **Mes pages** ou **Pages partagées** .

Que faire ensuite

Répétez cette procédure pour créer et gérer d'autres pages de graphiques ou de tableaux.

Pour des instructions sur la création d'une table à l'aide des commandes de clavier au lieu des clics de souris, voir «Exemple de création d'une table personnalisée avec les commandes du clavier», à la page 1143.

Exemple de création d'une table personnalisée avec les commandes du clavier

Les utilisateurs malvoyants peuvent utiliser l'onglet de tableau de bord **Détails d'attribut** pour créer des tables historiques comme alternative aux graphiques en courbes historiques, que les technologies d'assistance aux personnes handicapées, telles le logiciel de lecteur d'écran, ne peuvent pas interpréter.

Pourquoi et quand exécuter cette tâche

L'exemple suivant illustre l'utilisation des commandes du clavier pour créer une table historique des transactions qui sont signalées par l'Agent Synthetic Playback. Pour plus d'informations sur l'agent, voir «Gestion des transactions et des événements synthétiques», à la page 1058.

A mesure que vous appuyez sur la touche de tabulation, le focus se déplace en direction de la zone ou de la section suivante de la fenêtre d'application, de gauche à droite ou de haut en bas. Vous pouvez suivre ces étapes pour générer une table de transactions pour l'Agent de surveillance des temps de réponse en remplaçant My transactions par une application qui inclut l'agent, ou pour générer une table pour une instance de composant en remplaçant My transactions par une autre application et en sélectionnant le groupe Composants.

Procédure

Pour créer une table des transactions de l'Agent Synthetic Playback sous l'onglet **Détails d'attribut** à l'aide des raccourcis-claviers, procédez comme suit :

1. Connectez-vous à IBM Cloud Application Performance Management. Le focus se trouve sur la barre de navigation.
2. Pour ouvrir le Tableau de bord d'Application Performance, appuyez sur la flèche vers le bas pour déplacer le focus vers le menu **Performance**, appuyez sur la touche Entrée pour le sélectionner, appuyez sur la flèche vers le bas jusqu'à l'option **Tableau de bord d'Application Performance**, puis appuyez de nouveau sur la touche Entrée.
3. Pour ouvrir la page du tableau de bord Transactions synthétiques, appuyez plusieurs fois sur la touche de tabulation (environ 7 fois) jusqu'à ce que le focus se déplace vers le navigateur, puis appuyez sur la flèche vers le bas pour activer l'application prédéfinie My transactions et appuyez sur la touche Entrée.
4. Pour ouvrir la page du tableau de bord Détails des transactions, appuyez plusieurs fois sur la touche de tabulation (environ 10 fois) jusqu'à ce que le focus se déplace vers la section Instances de navigateur sur une instance de transaction de l'application Transactions Synthétiques, puis appuyez sur la touche Entrée. L'onglet **Détails d'attribut** apparaît sur le tableau de bord.
5. Pour ouvrir l'onglet **Détails d'attribut**, appuyez plusieurs fois sur la touche de tabulation (environ 6 fois) jusqu'à le focus se trouve sur l'onglet **Présentation des statuts**, puis appuyez sur la flèche vers la droite jusqu'à ce que le focus se trouve sur l'onglet **Détails d'attribut**. La **table**  **historique** ainsi que tous les attributs de l'ensemble de données Disponibilité des transactions dans le temps sont sélectionnés.
6. Pour générer la table, appuyez plusieurs fois sur la touche de tabulation (environ 18 fois) jusqu'à ce que le focus se trouve sur le bouton **Prévisualiser les résultats**, puis appuyez sur la touche Entrée.

Résultats

Les attributs Disponibilité des transactions dans le temps sont affichés dans une table, avec une colonne pour chaque attribut et une ligne pour chaque échantillon de données recueilli au cours des dernières 4 heures.

Que faire ensuite

- Pour diminuer le nombre de lignes affichées, vous pouvez appuyer sur la touche de tabulation pour activer la zone de texte Filtrer et saisir un texte partiel ou entier ou une valeur d'horodatage sur laquelle appliquer le filtre.

- Pour modifier l'intervalle, déplacez le focus vers le menu déroulant **Dernières 4 heures** du sélecteur de temps et sélectionnez une autre option. Pour plus d'informations, voir l'étape 11, à la page 1141 dans «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1140.
- Pour générer une table avec l'ensemble de données Temps de réponse de transaction, appuyez plusieurs fois sur la touche de tabulation (environ 2 fois) pour déplacer le focus ver l'outil **Nouveau**, puis appuyez sur la touche Entrée. Le panneau de sélection est affiché. Sélectionnez l'ensemble de données Temps de réponse de transaction et le bouton **Prévisualiser les résultats**.

Définition d'un filtre de tableau

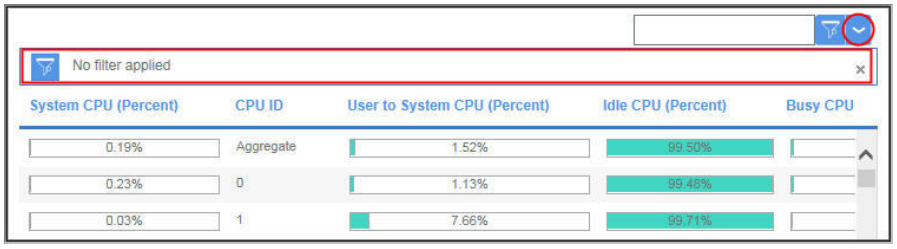
Vous pouvez limiter les lignes d'un tableau que vous visualisez dans l'onglet **Détails d'attribut** du tableau de bord pour n'afficher que les lignes d'un certain type, ou ayant des valeurs d'attribut spécifiques par texte ou par horodatage. Bien que les valeurs numériques soient indisponibles pour le filtrage, telles que les pourcentages, certaines valeurs d'attribut numérique sont converties en valeur d'affichage pour le tableau et traitées comme du texte.

Vous pouvez appliquer un filtre rapide ou ouvrir un éditeur pour composer un filtre avancé.

Procédure

Procédez comme suit pour filtrer un tableau personnalisé selon les valeurs d'attribut de texte ou d'horodatage. Bien que les valeurs numériques soient indisponibles pour le filtrage, telles que les pourcentages, certaines valeurs d'attribut numérique sont converties en valeur d'affichage pour le tableau et traitées comme du texte.

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, accédez au niveau d'une instance de la ressource gérée.
2. Cliquez sur l'onglet **Détails d'attribut**. La page enregistrée la plus récente est affichée ou, si aucune page n'a été enregistrée, les listes de sélection d'**Ensemble de données** et d'**Attributs** sont affichées.
3. Si une page de table enregistrée est affichée, passez à l'étape 5, sélectionnez une autre page de table enregistrée dans le menu déroulant ou cliquez sur **Ajouter** pour créer un nouveau tableau.
4. Si vous créez un nouveau tableau ou que vous éditez un tableau enregistré, sélectionnez l'**Ensemble de données** et les **Attributs** à utiliser, puis cliquez sur **Prévisualiser les résultats**.
5. Pour appliquer un filtre rapide, cliquez dans la zone de texte Filtre et entrez le texte partiel ou complet qui servira de filtre. A mesure que vous entrez des caractères, toutes les lignes ne contenant pas les caractères saisis sont supprimées du tableau. Pour supprimer le filtre rapide, supprimez la valeur ou cliquez sur «x».
6. Pour appliquer un filtre avancé, cliquez sur le menu déroulant et sélectionnez **Définir le filtre** ou cliquez dans la barre de filtre. La fenêtre de génération de filtre s'ouvre avec les règles qui ont été définies.



7. Pour définir une règle, renseignez les zones :
   a. Laissez le paramètre de colonne défini sur «Any Column» (Toute colonne) ou sélectionnez l'attribut selon lequel filtrer dans la liste.
   b. Laissez la condition définie sur «contains» (contient) ou sélectionnez un autre opérateur dans la liste et entrez la valeur de texte ou d'horodatage selon laquelle filtrer dans la zone de texte :

Condition	Ligne incluse dans le tableau lorsque...
contains	La valeur de filtre est trouvée quelque part dans la cellule.
equals	La valeur de cellule correspond exactement à la valeur de filtre, y compris la casse.
starts with	La valeur de cellule commence par les mêmes caractères que la valeur de filtre.
ends with	La valeur de cellule comporte les mêmes caractères que la fin de la valeur de filtre.
does not equal	La valeur de cellule n'est pas une correspondance exacte de la valeur de filtre.
does not contain	La valeur de cellule ne contient pas le même texte ou nombre que la valeur de filtre.
does not start with	La valeur de cellule ne commence pas par les mêmes caractères que la valeur de filtre.
does not end with	La valeur de cellule ne se termine pas par les mêmes caractères que la valeur de filtre.
is empty	La cellule ne contient pas de données.

c. Une fois que vous avez terminé la règle, cliquez sur **Filtre** pour voir les résultats, cliquez sur **Ajouter une règle de filtrage** pour ajouter une autre règle, ou passez à l'étape suivante.

8. Si le filtre comporte plusieurs règles, opérez votre sélection parmi les options suivantes :
   - **Match**(Correspondance) est défini initialement sur **All rules** (toutes les règles), ce qui signifie qu'une ligne s'affiche uniquement si ses données suivent toutes les règles du filtre. La ligne est exclue si aucune valeur de texte ou d'horodatage ne suit une règle. S'il existe plusieurs règles et que vous voulez inclure une ligne si elle suit l'une des règles au moins, remplacez le paramètre par **Any rule**.
   - Pour éditer une règle, modifiez une ou plusieurs valeurs de zone.
   - Pour supprimer une règle, sélectionnez-la et cliquez sur **Supprimer la règle**.
9. Lorsque vous avez terminé de définir une ou plusieurs règles, cliquez sur **Filtre** pour fermer la boîte de dialogue et appliquer le filtre.

Résultats

Les groupes qui ne répondent pas aux critères de filtrage ne s'affichent plus et la barre de filtre signale le nombre d'éléments, par exemple, «480 of 1200 items shown».

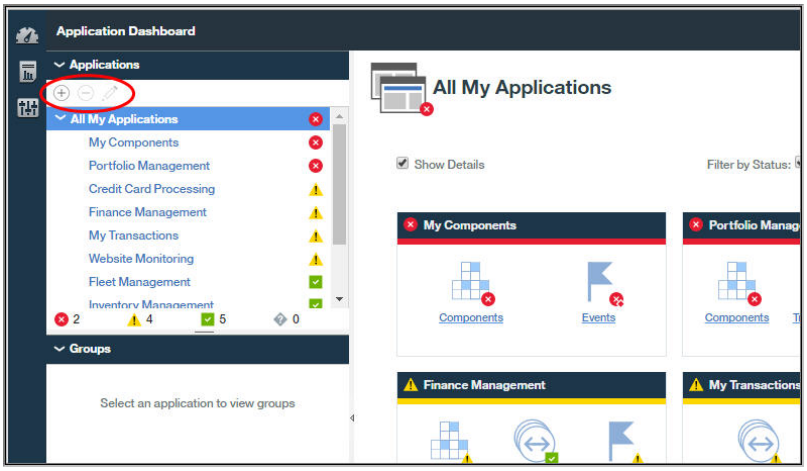
Que faire ensuite

- Survolez la barre de filtre avec le pointeur de la souris pour ouvrir une fenêtre en incrustation avec les critères de filtrage. Vous pouvez supprimer une règle (cliquez sur ×) ou cliquer à l'intérieur de la fenêtre pour éditer les critères de filtrage.
- Cliquez sur **Effacer le filtre** dans la barre de filtre ou sur **Effacer** dans la fenêtre Générer le filtre pour supprimer le filtre et afficher toutes les lignes.

Gestion des applications

Utilisez les outils disponibles dans le Tableau de bord d'Application Performance pour organiser vos ressources gérées dans les applications.

Les outils **Applications** du navigateur ouvrent l'éditeur d'application en vue de la création ou de l'édition d'applications et de l'application des ressources gérées disponibles.



L'application **Mes composants** est une application prédéfinie qui inclut les systèmes gérés reconnus par le serveur serveur Cloud APM. Elle ne peut pas être éditée ni supprimée.

Pour une démonstration vidéo sur l'ajout d'une application, visionnez Application Performance Management - Define Application.

Pour un scénario sur la création d'une application de surveillance de la liste d'applications IBM Java, voir «Ajout d'applications Web au Tableau de bord d'Application Performance», à la page 99 et «Association d'une Liste d'applications Java IBM à l'application Web», à la page 100.

Restriction : Vous devez disposer des droits de modification pour les Applications afin de pouvoir utiliser l'outil Ajouter une application. Vous devez disposer des droits de modifications pour Applications ou pour l'application spécifique afin de pouvoir utiliser les outils Supprimer et Editer. Pour plus d'informations, voir «Utilisation des rôles, des utilisateurs et des droits», à la page 1027.

Ajout d'une application

Utilisez l'éditeur d'application pour créer une application et appliquer les ressources gérées qui sont disponibles, ou sélectionner une application parmi les applications reconnues.

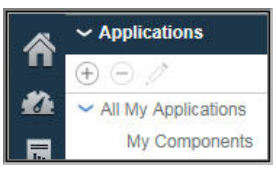
Avant de commencer

Vous devez disposer des droits de modification pour les Applications afin de pouvoir utiliser l'outil Ajouter une application. Pour plus d'informations, voir «Utilisation des rôles, des utilisateurs et des droits», à la page 1027.

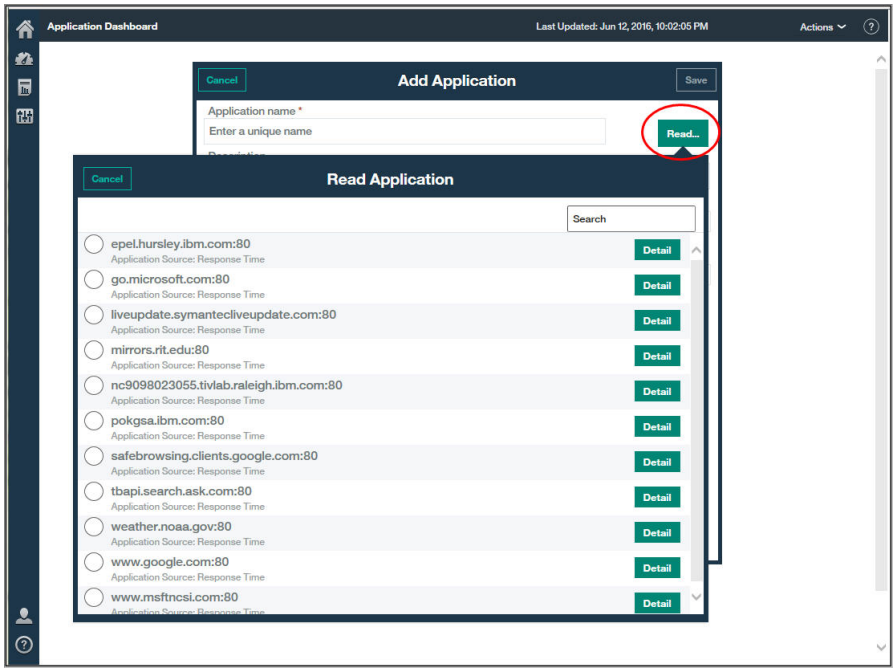
Procédure

Effectuez les étapes suivantes dans la console Cloud APM pour ajouter une application au Tableau de bord d'Application Performance.

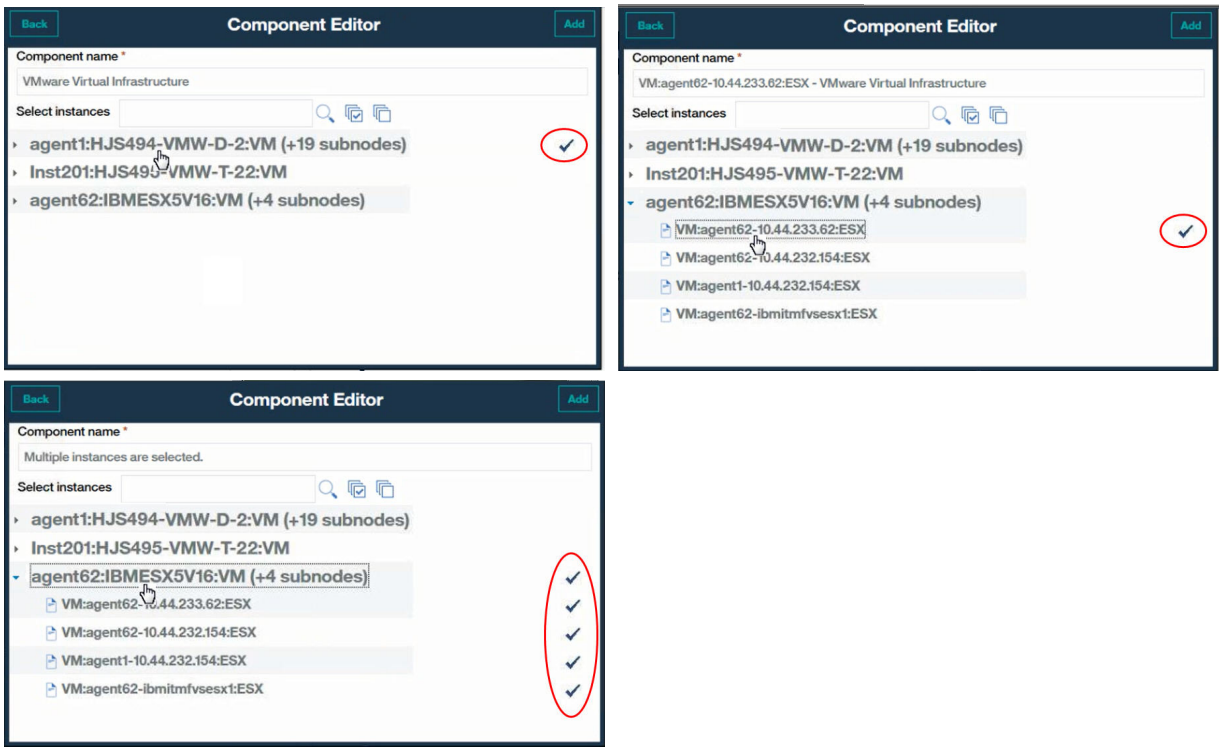
1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.
2. Dans la section Applications du navigateur, cliquez sur . La fenêtre Ajouter une application s'ouvre.



3. Entrez un nom pour votre application dans la zone **Nom de l'application** ainsi qu'une description (facultatif) dans la zone **Description**. N'utilisez pas les symboles `! " % & ' * ? < > } { \` dans le nom ou la description. Des exemples de nom d'application tels que «Finance Management» et «Credit Card Processing» sont disponibles dans la Démonstration guidée.
4. Cliquez sur **Lire** pour ouvrir la fenêtre Lire l'application affichant la liste des applications reconnues et effectuez une ou plusieurs des étapes ci-après :
   - Cliquez sur **Détail** pour afficher les composants d'une application.
   - Sélectionnez l'application que vous voulez utiliser, puis cliquez sur **Sauvegarder**. La fenêtre Lire l'application se ferme, le référentiel source apparaît dans la zone **Application lue dans**, et les composants sont répertoriés dans **Composants d'application**.
   - Cliquez sur **Annuler** pour fermer la fenêtre sans effectuer de choix.



5. Dans la zone **Modèle**, conservez le modèle Application personnalisée ou sélectionnez un modèle différent avec le bouton ›, puis cliquez sur **Sauvegarder**. Les instances et les types de composant associés sont répertoriés dans la liste **Composants d'application**.
6. Cliquez sur ⊕ **Ajouter des composants** et, dans la fenêtre Sélectionner le composant qui s'ouvre, sélectionnez un composant dans la liste. L'éditeur de composant s'ouvre.
7. Pour rechercher et sélectionner des instances de noeud et/ou de sous-noeud agent pour l'application, effectuez une ou plusieurs des étapes ci-après :
   - Cliquez sur une instance pour la sélectionner.
   - Pour les noeuds agent comportant des sous-noeuds, sélectionnez le noeud seul en cliquant sur son nom dans l'arborescence alors que celle-ci est réduite, sélectionnez le noeud et tous les sous-noeuds en développant l'arborescence de noeud (cliquez sur ▸), puis cliquez sur le noeud, ou sélectionnez des sous-noeuds individuels en développant l'arborescence de noeud et en cliquant sur l'instance.
   - Utilisez la barre d'outils pour rechercher des instances contenant le texte dans la zone de texte à rechercher, sélectionner toutes les instances, ou désélectionner toutes les instances.
   - Pour changer le nom d'affichage dans le navigateur, éditez le nom du composant.



V6-V7 Si vous ajoutez une instance d'agent Tivoli Monitoring et ne le voyez pas dans la liste des instances disponibles, vérifiez que Tivoli Enterprise Portal Server qui est associé à la Passerelle hybride est dans une version prise en charge (visitez le Hybrid Gateway supported agents (APM Developer Center)).

8. Cliquez sur **Ajouter** pour ajouter les noeuds et sous-noeuds agent sélectionnés à l'application, puis cliquez sur **Précédent**. La liste Composants d'application est mise à jour avec les nouveaux noms de composant.
9. Sélectionnez un autre composant auquel ajouter des instances, puis répétez les étapes 6, à la page 1147, 7, à la page 1147 et 8, ou cliquez sur **Fermer**.
10. Si d'autres instances sont liées aux composants dans la liste **Composants d'application**, un bouton qui indique le nombre d'instances liées est affiché, et vous pouvez effectuer les opérations suivantes :
    a. Cliquez sur le bouton (1) pour afficher les instances associées dans la fenêtre Détails mis à jour. Une barre s'affiche pour chaque type de mise à jour, y compris le nom d'instance. Par exemple, si l'un des composants a été supprimé, il apparaît sous la barre des composants Supprimé.
    b. Sélectionnez une ou plusieurs instances et cliquez sur **Sauvegarder** pour mettre à jour la liste des ressources d'application.
11. Une fois que vous avez terminé de définir l'application, fermez l'éditeur d'application en cliquant sur **Sauvegarder** pour sauvegarder vos modifications, ou cliquez sur **Annuler** pour annuler les modifications.

Résultats

Vos mises à jour d'application sont effectuées par le serveur Cloud APM une fois que vous avez sauvegardé vos modifications. L'affichage des modifications dans le tableau de bord peut prendre quelques minutes. (Essayez de nettoyer le cache du navigateur si l'affichage de vos modifications prend trop de temps.) La nouvelle application s'affiche dans le Tableau de bord d'Application Performance et dans la section Applications du navigateur. Lorsque l'application est sélectionnée, les composants s'affichent dans la section Groupes.

Edition d'une application

Utilisez l'éditeur d'application pour modifier une application définie et ajouter ou supprimer des ressources gérées en tant que composants de l'application.

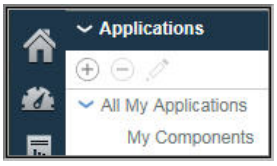
Avant de commencer

Vous devez disposer d'une autorisation de modification des applications ou de l'application spécifique pour utiliser l'outil d'édition. Pour plus d'informations, voir «Rôles et droits», à la page 1021.

Procédure

Effectuez les étapes suivantes dans la console Cloud APM pour éditer une application.

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.
2. Sélectionnez l'application à éditer dans la liste Toutes mes applications du navigateur, puis cliquez sur .

   La fenêtre Modification d'application s'ouvre.
3. Facultatif : Editez le **Nom d'application** ou la **Description**. N'utilisez pas les symboles `! " % & ' * ? < > } { \` dans le nom ou la description.
   Si vos autorisations d'affichage ou de modification des applications concernent certaines applications mais pas toutes, vous ne pourrez peut-être pas visualiser l'application dans le tableau de bord ni la modifier après son changement de nom. Cette limitation se produit car l'application renommée est traitée comme une nouvelle application. Demandez à l'administrateur de rôle ou de surveillance de vous donner l'autorisation d'affichage ou de modification de l'application renommée.
4. Pour ajouter des composants et des instances à l'application procédez comme suit.
   a. Cliquez sur et, dans la fenêtre qui s'ouvre, sélectionnez un composant dans la liste. L'éditeur de composant s'ouvre.
   b. Sélectionnez les instances de noeud et/ou de sous-noeud agent pour l'application :
      - Cliquez sur une instance pour la sélectionner.
      - Pour les noeuds comportant des sous-noeuds, sélectionnez le noeud en cliquant sur son nom dans l'arborescence alors que celle-ci est réduite, sélectionnez le noeud et tous les sous-noeuds en développant l'arborescence de noeud (cliquez sur), puis cliquez sur le noeud, ou sélectionnez des sous-noeuds individuels en développant l'arborescence de noeud et en cliquant sur l'instance.
      - Utilisez la barre d'outils pour rechercher des instances contenant le texte dans la zone de texte à rechercher, sélectionner toutes les instances, ou désélectionner toutes les instances.
      - Pour changer le nom d'affichage dans le navigateur, éditez le nom du composant.
   c. Cliquez sur **Ajouter** pour ajouter l'instance ou les instances, puis cliquez sur **Précédent**. La liste Composants d'application est mise à jour avec les nouveaux noms de composant.
   d. Vous pouvez sélectionner un autre composant auquel ajouter des instances, ou cliquer sur **Fermer**.

   La liste Composants d'application est mise à jour avec les nouveaux noms de composant. Le nombre entre parenthèses après le nom correspond au nombre d'instances qui sont associées au composant.
5. Pour éditer un nom de composant ou changer l'instance qui lui est associée, sélectionnez le composant dans la liste **Composants d'application** et cliquez sur :

a. Pour associer une autre instance au composant, recherchez l'instance de votre choix et sélectionnez-la.
b. Pour changer le nom de composant qui est utilisé comme nom d'affichage dans le navigateur pour cette application, éditez la zone de **nom du composant**.
c. Cliquez sur **Save**.

La liste Composants d'application est mise à jour avec les modifications que vous avez apportées.

6. Pour retirer un composant ou une instance de l'application, sélectionnez-le ou la et cliquez sur . Cliquez sur **OK** pour confirmer.
7. Si d'autres instances sont liées aux composants dans la liste **Composants d'application**, un bouton qui indique le nombre d'instances liées est affiché, et vous pouvez effectuer les opérations suivantes :
   a. Cliquez sur le bouton pour afficher les instances associées dans la fenêtre Détails mis à jour. Une barre s'affiche pour chaque type de mise à jour, y compris le nom d'instance. Par exemple, si l'un des composants a été supprimé, il apparaît sous la barre des composants Supprimé.
   b. Sélectionnez une ou plusieurs instances et cliquez sur **Sauvegarder** pour mettre à jour la liste des ressources d'application.
8. Une fois que vous avez terminé d'éditer l'application, fermez l'éditeur d'application en cliquant sur **Sauvegarder** pour sauvegarder vos modifications, ou cliquez sur **Annuler** pour annuler les modifications.

Résultats

Vos mises à jour d'application sont effectuées par le serveur Cloud APM une fois que vous avez sauvegardé vos modifications. L'affichage des modifications dans le tableau de bord peut prendre quelques minutes.

Référence associée:

«Rôles et droits», à la page 1021
Un *rôle* est un groupe de droits qui contrôle les actions que vous pouvez effectuer dans Cloud APM.

Suppression d'une application

Lorsque vous n'en n'avez plus besoin, vous pouvez supprimer une application dont vous avez défini l'affichage dans le Tableau de bord d'Application Performance.

La suppression d'une application ne désinstalle pas les composants de prise en charge ; seule l'application qui les contient est supprimée. Ces mêmes composants peuvent être ajoutés à d'autres applications et ne sont pas supprimés des applications auxquelles ils appartiennent.

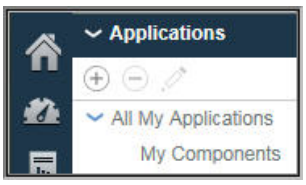
Avant de commencer

Vous devez disposer des droits de modification pour Applications ou pour l'application spécifique pour pouvoir utiliser l'outil Supprimer. Pour plus d'informations, voir «Utilisation des rôles, des utilisateurs et des droits», à la page 1027.

Procédure

Pour supprimer une application du Tableau de bord d'Application Performance, procédez comme suit :

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.



2. Dans la section Applications du navigateur, sélectionnez l'application que vous voulez supprimer de la liste Toutes mes applications, puis cliquez sur . Un message vous demandant de confirmer votre choix s'affiche.
3. Cliquez sur **Oui** pour confirmer la suppression de l'application, ou sur **Non** si vous n'êtes pas sûr de votre choix.

Résultats

Une fois que vous avez cliqué sur **Oui**, l'application est supprimée du Tableau de bord d'Application Performance.

Que faire ensuite

Répétez cette étape pour les autres applications à supprimer.

Affichage et suppression des agents en ligne

Les agents hors ligne pendant quatre jours sont supprimés de la console Cloud APM. Cette rubrique décrit la façon dont les agents hors ligne sont indiqués, ainsi que l'impact sur les groupes de ressources, les vues de topologie et les autres fonctions. Pour supprimer un système géré du tableau de bord avant la période des quatre jours, utilisez l'éditeur d'application. Vous pouvez également définir un délai avant suppression pour les systèmes gérés hors ligne..

Pourquoi et quand exécuter cette tâche

Une fois les agents installés sur les systèmes que vous voulez gérer, ils se connectent au serveur Cloud APM et envoient des échantillons de données au Tableau de bord d'Application Performance à des fins de présentation et d'évaluation des seuils. Si un agent est hors ligne, l'indicateur de statut s'affiche dans le navigateur et le tableau de bord. Si, au bout d'un certain temps, l'agent ne répond pas, le serveur affiche un message indiquant que l'agent est indisponible. Voir «Exemples d'agents hors ligne», à la page 1152.

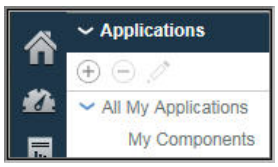
Après quatre jours, l'agent hors ligne est supprimé de l'interface utilisateur, sauf s'il prend en charge le suivi des transactions. Dans ce cas, l'agent hors ligne continue de s'afficher dans les vues Agréger une topologie de transaction et Topologie des instances de transaction.

Vous pouvez supprimer l'agent hors ligne des applications définies ; il est alors supprimé de la console Cloud APM avant que la période des quatre jours ne soit totalement écoulée. Vous pouvez également définir le délai avant suppression d'un agent hors ligne de la vue, dans le cadre d'une future occurrence. Voir la section «Et ensuite ?» en fin de rubrique.

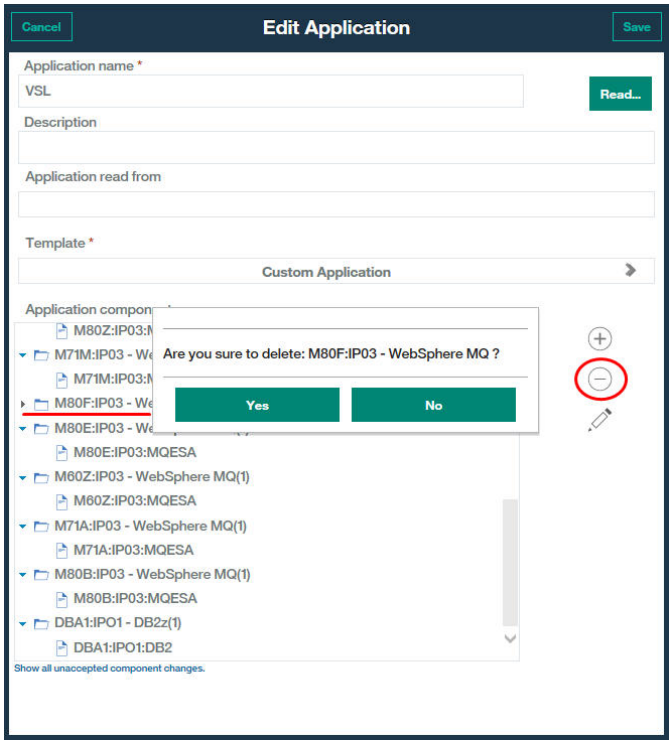
Procédure

Pour supprimer un agent hors ligne d'une application définie, procédez comme suit :

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.
2. Dans la section Applications du navigateur, sélectionnez l'application à laquelle l'agent hors ligne appartient, puis cliquez sur **Modifier une application**.



3. Sélectionnez l'agent ou le sous-noeud agent dans la liste Composants d'application, puis cliquez sur . Pour les agents comportant des sous-noeuds, sélectionnez l'agent seul en cliquant sur son nom dans l'arborescence alors que celle-ci est réduite, sélectionnez le noeud et tous les sous-noeuds en développant l'arborescence de noeud (cliquez sur), puis cliquez sur le noeud, ou sélectionnez des sous-noeuds individuels en développant l'arborescence de noeud et en cliquant sur l'instance.



4. Une fois que vous avez modifié l'application en vue de supprimer l'agent ou le sous-noeud hors ligne, cliquez sur **Sauvegarder**.

Résultats

Vos mises à jour d'application sont effectuées par le serveur Cloud APM une fois que vous avez sauvegardé vos modifications. La suppression de l'agent hors ligne du Tableau de bord d'Application Performance peut prendre quelques minutes.

Que faire ensuite

Vous pouvez régler le paramètre **Délai avant suppression d'un système hors ligne** au niveau de la page **Configuration avancée** pour augmenter ou réduire le délai avant suppression de l'agent hors ligne dans le cadre de la vue. Pour plus d'informations, voir «Fonction d'abonnement d'agent», à la page 1121.

Exemples d'agents hors ligne

Cette rubrique décrit les modes d'affichage possibles des agents hors ligne dans la console Cloud APM. Vous pouvez supprimer l'affichage des agents hors ligne que vous ne voulez plus surveiller.

La surveillance reprend si l'agent se remet en ligne.

Lorsqu'un agent est hors ligne, aucune donnée n'est envoyée à la console console Cloud APM et le Tableau de bord d'Application Performance affiche un indicateur de statut pour l'agent et pour les applications auxquelles il appartient. L'agent ne peut pas être ajouté à une application définie de l'éditeur d'application ni à un groupe personnalisé du gestionnaire de groupes de ressources, de même qu'il ne peut pas créer de tableaux et de graphiques à courbes d'historique dans l'onglet Détails d'attribut.

Tableau de bord d'Application Performance - Toutes mes applications

La page d'accueil de tableau de bord Toutes mes applications fournit la première indication quant au statut hors ligne. Le compteur situé dans la section Applications du navigateur indique le nombre d'applications dont les ressources sont indisponibles.

La zone récapitulative indique le statut d'événement Normal, aucun événement n'étant ouvert pour les ressources gérées de l'application.

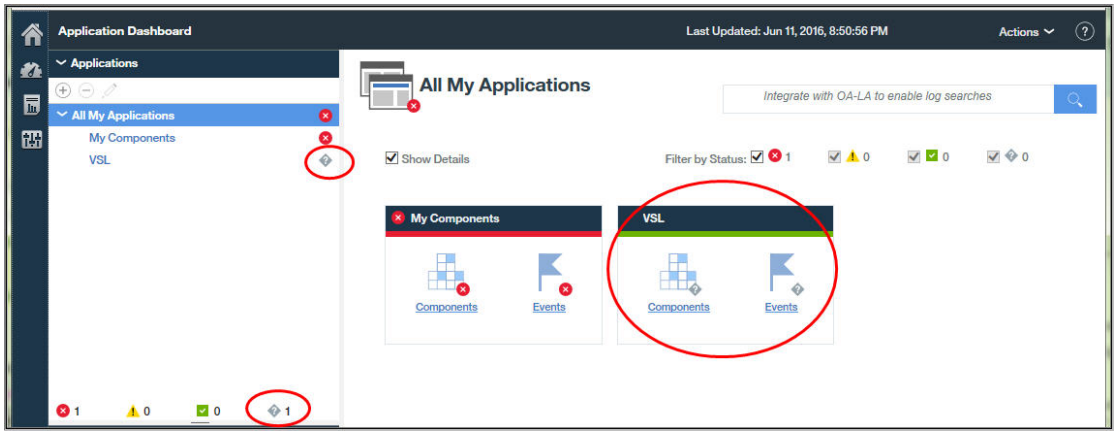


Tableau de bord d'Application Performance - Application

Une fois que l'utilisateur a cliqué sur la barre de titre de la zone récapitulative ou a sélectionné l'application depuis le navigateur, l'onglet Présentation des statuts s'affiche avec un graphique Récapitulatif de la gravité de l'événement vide. Le graphique à barres Statut du composant en cours indique le statut «Inconnu» pour les agents hors ligne.

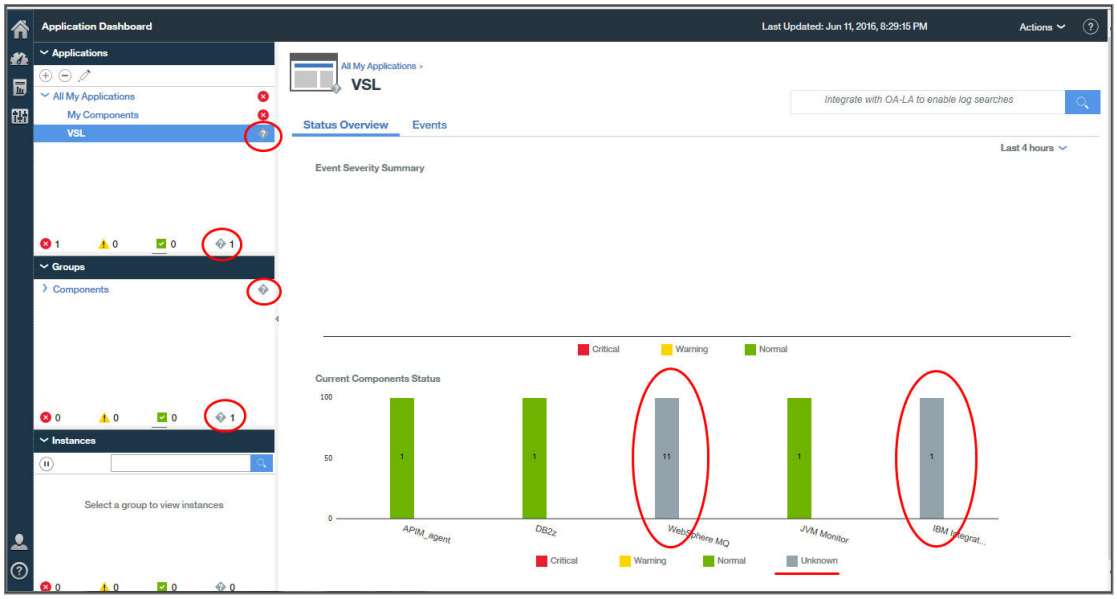


Tableau de bord d'Application Performance - Groupe

Une fois que l'utilisateur a cliqué sur le graphique Statut de composant en cours ou sur le groupe Composants du navigateur, l'onglet Présentation des statuts est modifié et affiche un widget de groupe récapitulatif pour chaque ressource gérée. Les widgets de groupe des agents non

disponibles affichent un message indiquant que l'agent est hors ligne au lieu des indicateurs clés de performance.

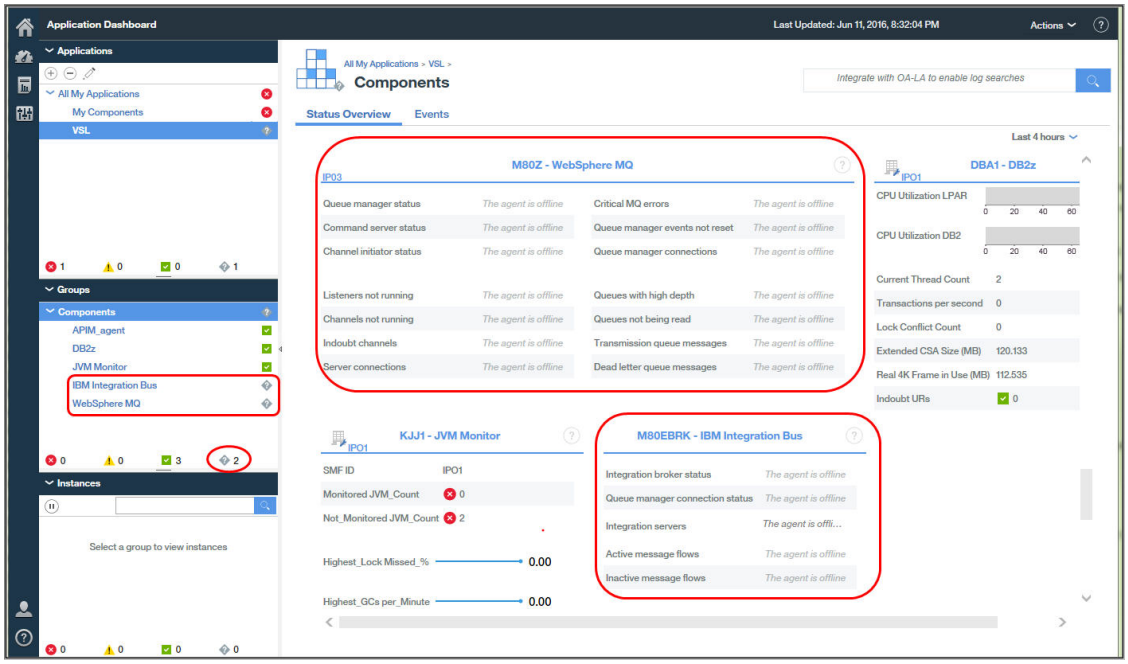
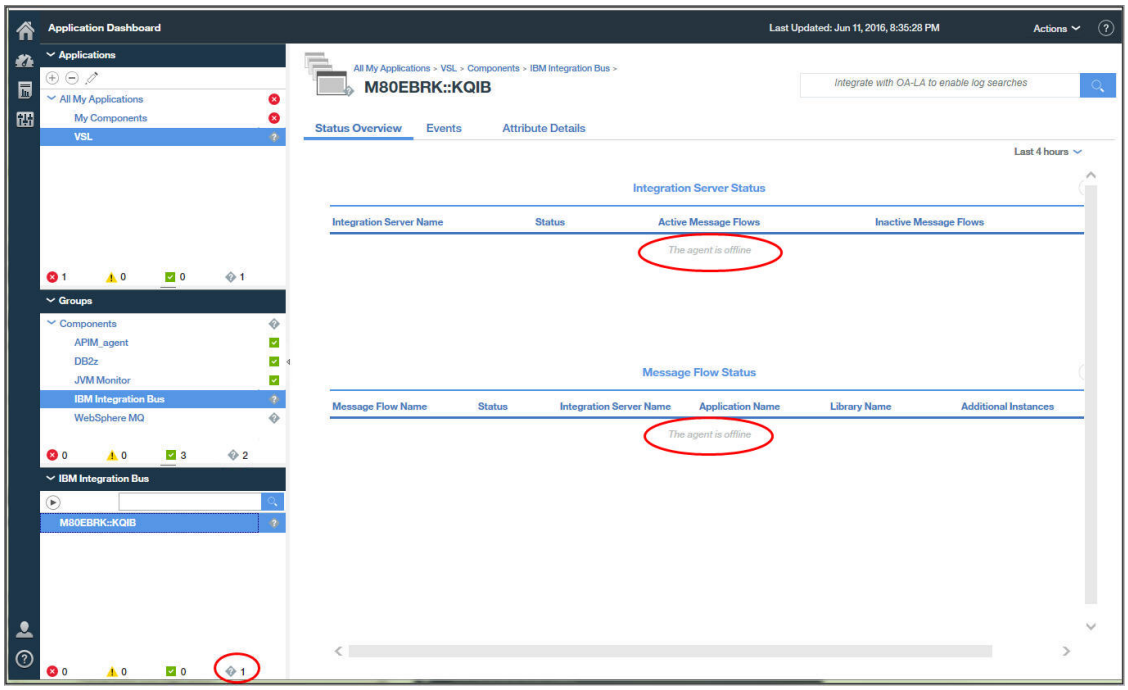


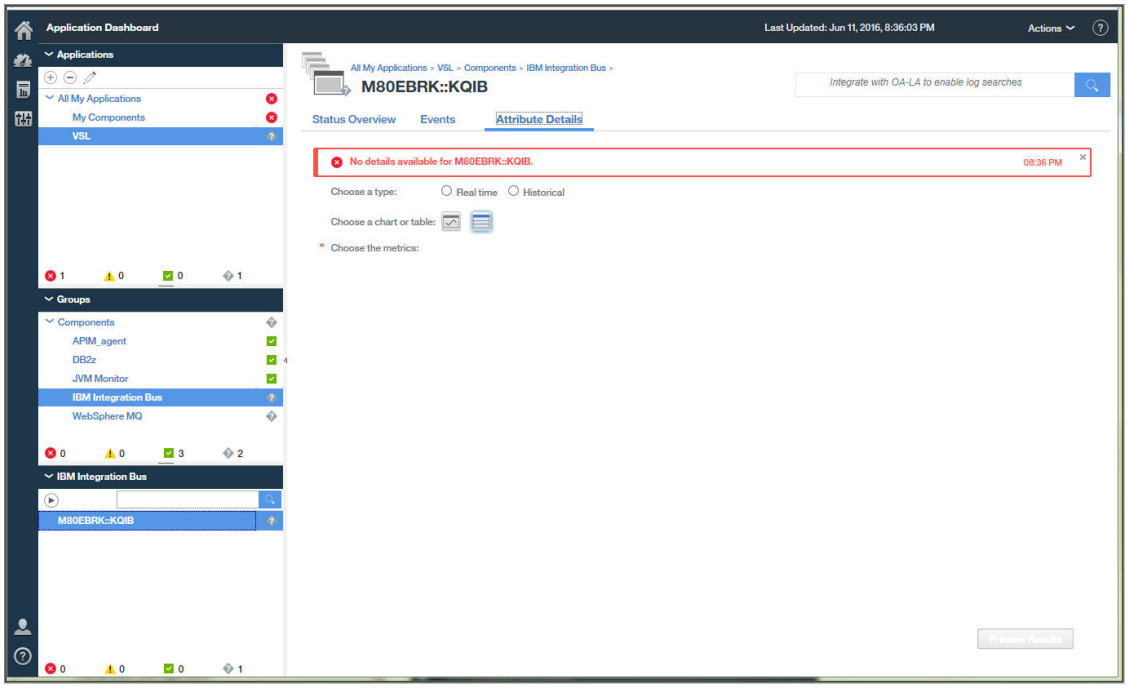
Tableau de bord d'Application Performance - Instance

Une fois que l'utilisateur a cliqué sur l'un des widgets de groupe récapitulatif de l'agent hors ligne, l'onglet Présentation des statuts affiche des widgets de table et de graphique pour l'agent sélectionné. Cependant, comme pour le widget de groupe récapitulatif, seul le message indiquant que l'agent est hors ligne s'affiche, au lieu des indicateurs clé de performance pour l'instance d'agent.



Lorsque l'utilisateur clique sur l'onglet Détails d'attribut, un message indiquant qu'aucun détail n'est disponible pour l'instance d'agent s'affiche. Il n'est pas possible de créer un graphique ou un

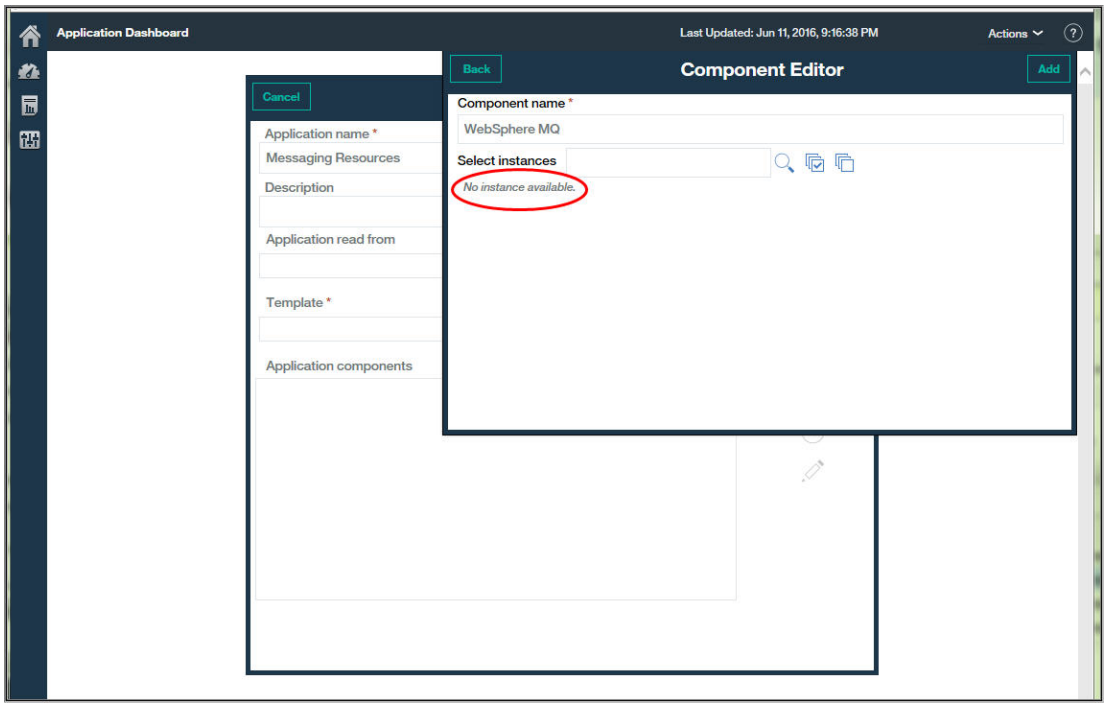
tableau personnalisé pour l'instance d'agent hors ligne.



Editeur d'application

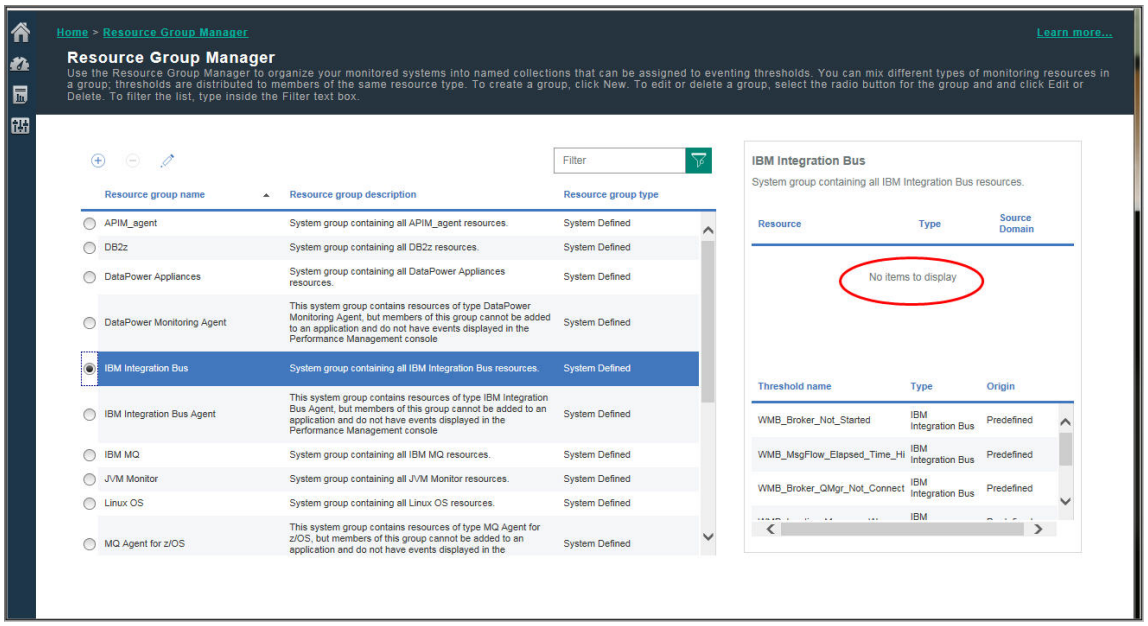
Dans le Tableau de bord d'Application Performance, lorsque l'utilisateur clique sur l'outil **Ajouter une application** ou **Modifier une application** de la section Applications du navigateur, la fenêtre d'éditeur d'application apparaît.

Lorsque l'utilisateur clique sur **Ajouter des composants** et qu'il sélectionne un type d'agent, si aucun agent de ce type n'est installé ou qu'un agent est hors ligne, un message indiquant qu'aucune instance d'agent n'est disponible s'affiche. Si d'autres instances d'agent sont disponibles, elles sont répertoriées dans la liste.



Gestionnaire de groupes de ressources

Lorsque l'utilisateur sélectionne **Configuration du système** > **Gestionnaire de groupes de ressources**, la page s'affiche avec une table des groupes de ressources. Lorsque vous sélectionnez un groupe, les instances d'agent qui le composent sont répertoriées avec les seuils affectés. Si toutes les instances d'agent sont hors ligne, un message indiquant qu'aucune instance n'est disponible s'affiche.



Concepts associés:

«Gestion des applications», à la page 1145
Utilisez les outils disponibles dans le Tableau de bord d'Application Performance pour organiser vos ressources gérées dans les applications.

Chapitre 14, «Utilisation des tableaux de bord», à la page 1125
Sélectionnez **Performance** > **Tableau de bord d'Application Performance** pour obtenir une présentation complète du statut de vos applications. Vous pouvez effectuer une exploration en aval de la vue la plus générale à la vue détaillée des mesures, dans le même écran.

Référence associée:

«Gestionnaire de groupes de ressources», à la page 995
Votre environnement surveillé peut comporter plusieurs systèmes gérés pouvant être catégorisés par objectif. Ces systèmes possèdent souvent les mêmes exigences de seuil. Utilisez le gestionnaire de groupes de ressources pour organiser les systèmes gérés en groupes auxquels vous pouvez affecter des seuils. Vous pouvez également créer des groupes de ressources correspondant à vos stratégies de contrôle d'accès basé sur les rôles.

Statut de l'événement

Utilisez le Statut de l'événement pour obtenir une présentation récapitulative des événements ouverts de l'élément de navigateur sélectionné et pour répondre aux événements ayant le statut critique ou avertissement en accédant aux tableaux de bord détaillés.

Les indicateurs de statut concernent les événements de seuil qui sont exécutés sur vos systèmes gérés. Si des Passerelles hybrides sont configurées, les événements peuvent également être déclenchés par des situations survenant sur les systèmes gérés de votre environnement IBM Tivoli Monitoring. Si votre configuration inclut IBM Operations Analytics - Predictive Insights, toute anomalie détectée est également affichée.

Les événements liés à certains seuils ne sont pas affichés dans le Tableau de bord d'Application Performance. Les seuils utilisent des attributs pour des ressources qui ne sont pas publiées, ce qui peut se produire dans les agents prenant en charge des sous-noeuds. (Pour une description des sous-noeuds, voir la rubrique Agent Builder à l'adresse).

Critique, Avertissement, Normal

- Les indicateurs de statut consolident les gravités d'événement à partir des seuils :

  Le statut Critique indique tous les événements dont la gravité est Fatal ou Critique.

  Le statut Avertissement indique tous les événements ayant un niveau de gravité Mineur ou Avertissement.

  Le statut Normal indique tous les événements ayant un niveau de gravité Inconnu.

  Le statut Inconnu indique que le système géré est hors ligne. Après avoir passé 4 jours hors ligne, le système géré est supprimé de toutes les applications et n'apparaît plus dans les tableaux de bord.
  Pour vérifier le statut, arrêter ou démarrer un agent, voir «Utilisation des commandes de l'agent», à la page 213
  Pour modifier le temps d'attente avant qu'un système géré en mode hors connexion soit supprimé, voir l'option **Délai avant suppression d'un système hors ligne** dans «Fonction d'abonnement d'agent», à la page 1121
- V6-V7 Si une ou plusieurs Passerelles hybrides sont configurées, les indicateurs de statut des événements générés par les situations Tivoli Monitoring sont identiques à ceux des seuils, à l'exception du statut Normal qui indique des événements dont le niveau de gravité est Sans conséquences, Information ou Inconnu.
- Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights, toutes les anomalies détectées sont indiquées par une icône en forme de diamant sur l'indicateur de statut, par exemple . Pour plus d'informations, voir «Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights», à la page 1159.

Graphique Récapitulatif de la gravité de l'événement (%)

- Le graphique Récapitulatif de la gravité de l'événement présente les pourcentages de statut d'événement Critique, Avertissement et Normal. Par exemple,
  

  indique que 50 % des événements sont générés par des seuils de gravité Mineur ou Avertissement et 50 % des événements par des seuils de gravité Fatal ou Critique.
- Le nombre total d'événements est indiqué, ainsi que le nombre d'événements pour chaque niveau de statut.
- Le nombre d'événements inclut toutes les anomalies détectées par Operations Analytics - Predictive Insights. Par exemple, un total de «8 dont 1 anomalie» signifie qu'il existe 7 événements de seuil et 1 événement d'anomalie.

Tableau des événements

- Le tableau des événements ouverts et des statuts est défini par l'élément de navigateur sélectionné : application, groupe, sous-groupe ou instance.
- Les événements sont triés dans la colonne Gravité, en commençant par la gravité la plus élevée. Cliquez sur un en-tête de colonne pour modifier l'ordre de tri.
- Chaque ligne fournit les informations suivantes sur l'événement :

  Nom du seuil
  Nom qui a été attribué au seuil.

  V6-V7 Nom qui a été attribué à la situation.

  Statut Statut de l'événement, par exemple Ouvert.

  Gravité
  Valeur de gravité de l'événement : Critique (s'applique aux gravités de génération

d'événement Fatal et Critique), Avertissement (s'applique aux gravités de seuil de génération d'événement Mineur et Avertissement ou Normal (s'applique aux gravités de seuil Inconnu ; pour les événements Tivoli Monitoring, s'applique aux niveaux de gravité Sans conséquences, Information et Inconnu).

Le statut Inconnu indique que le système géré est hors ligne. Après avoir passé 4 jours hors ligne, le système géré est supprimé de toutes les applications et n'apparaît plus dans les tableaux de bord. (Pour vérifier le statut, arrêter et démarrer un agent, voir «Utilisation des commandes de l'agent», à la page 213.)
Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights, l'analyse appliquée aux données d'historique peut détecter une anomalie et ouvrir un événement. Un événement ouvert pour une anomalie détectée est indiqué par une icône recouvrant l'indicateur de statut, comme l'. Cliquez sur le lien **Afficher l'analyse des anomalies** pour ouvrir la vue Predictive Insights Service Diagnosis dans un nouvel onglet ou une nouvelle fenêtre de navigateur. Utilisez la vue Service Diagnosis pour examiner tout comportement anormal dans les composants qui prennent en charge l'application.

Elément affiché
S'applique uniquement à des ensembles de données à plusieurs lignes. L'élément d'affichage est un attribut clé qui a été sélectionné pour le seuil afin de différencier les événements qui ont été ouverts pour le même système géré.

Source
Nom d'hôte du système ou autre nom dérivé de l'agent de surveillance qui identifie la source de l'événement.

Horodatage
Date et heure de survenue de l'événement ou d'observation de la condition par l'agent émetteur, exprimées dans le fuseau horaire de l'utilisateur de la console Cloud APM.

Si un agent est redémarré ou si les définitions de seuil sont modifiées pour un agent, les événements échantillonnés de l'agent sont fermés et rouverts si la condition de seuil est toujours vraie. Dans ces scénarios, la valeur `Horodatage` est mise à jour pour indiquer l'heure à laquelle l'agent émetteur a rouvert l'événement.

Pour les événements purs, un nouvel événement est ouvert par l'agent et remplace l'instance d'événement précédente chaque fois que l'agent émetteur détermine que la condition de seuil est vraie. Un événement pur reste ouvert pendant 24 heures (ou un nombre d'heures configurable) après la dernière évaluation de la condition de seuil comme vraie. Seule l'instance la plus récente d'un événement pur est affichée sur la console Cloud APM.

Description
Description éventuelle du seuil.

- Cliquez sur une ligne pour développer les détails relatifs à l'événement :

Noeud
Nom du système géré de l'instance de noeud.

Pour les agents possédant des sous-noeuds, l'option **`Activer les événements sous-noeud`** contrôle si les sous-noeuds sont affichés, ou non. Pour plus d'informations, voir «Intégration de l'interface utilisateur», à la page 1117.

ID seuil
Identificateur de seuil.

Horodatage global
Date et heure auxquelles serveur Cloud APM a reçu l'événement de l'agent émetteur, exprimées dans le fuseau horaire de l'utilisateur de la console Cloud APM.

Type Indique si l'événement est pur ou échantillonné. Les événements purs sont des

notifications non sollicitées. Aucun intervalle d'échantillonnage n'est défini pour les seuils des événements purs et il n'est pas possible de surveiller les valeurs en cours d'une mesure constante.

Description
Description éventuelle du seuil.

Formule
Formule telle qu'elle est écrite dans l'éditeur de seuil. Par exemple, `Percent Failed > 10.000 AND Transaction Definition Name != 'Ignore_Resources'`.

IBM Cloud Application Performance Management 8.1.4.0 Interim Fix 3 Server Patch ou ultérieur (sur Fix Central) : si la fonction de Personnalisation de l'attribut EIF a été utilisée pour personnaliser la valeur de l'attribut de base **msg**, la valeur personnalisée de l'attribut **msg** s'affiche à la place de la formule de seuil. Pour plus d'informations, voir «Acheminer l'événement de fonction d'intégration d'événements ?», à la page 1003 sous la rubrique Gestionnaire de seuils et «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1007.

Vous pouvez sélectionner et développer d'autres lignes, ou cliquer de nouveau pour réduire une ligne. Tandis qu'une ligne est développée, vous pouvez effectuer une exploration en aval vers les tableaux de bord du système géré qui peuvent vous aider à déterminer la cause de l'événement.

Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights

IBM Cloud Application Performance Management uniquement :Si votre environnement géré inclut IBM Operations Analytics - Predictive Insights, l'analyse appliquée aux données d'historique peut détecter les anomalies et ouvrir des événements.

Le Tableau de bord d'Application Performance permet de localiser et de visualiser les anomalies détectées par Operations Analytics - Predictive Insights.

Avant de commencer

Operations Analytics - Predictive Insights doit être intégré à votre environnement Cloud APM pour que vous soyez alerté des anomalies dans le Tableau de bord d'Application Performance. Pour plus d'informations, voir «Intégration à Operations Analytics - Predictive Insights», à la page 908.

Pourquoi et quand exécuter cette tâche

Le Tableau de bord d'Application Performance présente le récapitulatif de statut des applications dans vos domaines ainsi que leurs systèmes gérés de composant. Les indicateurs de statut d'événement des zones récapitulatives du tableau de bord **Toutes mes applications** présentent des gravités de niveau Critique, Avertissement et Inconnu. Si les événements incluent des anomalies détectées par Operations Analytics - Predictive Insights, l'indicateur de statut inclut une icône d'anomalie : , ou . Cet indicateur, identique pour les anomalies d'avertissement et pour les anomalies critiques, apparaît à côté du titre de l'onglet d'**Evénements** à mesure que vous descendez dans la hiérarchie jusqu'aux pages de tableau de bord d'application, de groupe et d'instance : Events 2. Pour accéder à une démonstration pratique, démarrez la Démonstration guidée du produit IBM Cloud Application Performance Management, défilez jusqu'à la liste des tâches, puis sélectionnez *Identify & Diagnose Predictive Insights Anomalies*.

Procédure

Pour identifier des anomalies et les afficher dans la vue Service Diagnosis d'Operations Analytics - Predictive Insights, procédez comme suit :

1. Cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**.
2. Si une zone récapitulative contient un indicateur de statut **Evénements** qui présente une icône d'anomalie, cliquez sur le lien **Evénements**. Le Tableau de bord des applications s'ouvre dans l'onglet **Evénements**. Le Récapitulatif de la gravité de l'événement indique le nombre total d'événements, y compris le nombre d'anomalies.
3. Cliquez sur une ligne de table contenant un événement d'anomalie qui est indiqué dans la colonne Gravité par , ou . La ligne se développe pour afficher les détails d'événement.
4. Cliquez sur **Afficher l'analyse des anomalies** pour ouvrir la vue Service Diagnosis d'Operations Analytics - Predictive Insights dans un nouvel onglet ou une nouvelle fenêtre de navigateur.

Que faire ensuite

- Utilisez la vue Service Diagnosis pour examiner tout comportement anormal dans les composants qui prennent en charge l'application. Cliquez sur pour ouvrir l'aide en ligne pour la vue Service Diagnosis.
- Revenez au Tableau de bord des applications et recherchez d'autres événements sur le système géré pouvant indiquer un problème associé. Cliquez sur l'onglet **Présentation des statuts** et accédez à l'instance du système géré sur laquelle l'événement s'est produit pour procéder à une recherche plus approfondie. Utilisez les informations pour déterminer quelles actions doivent être prises pour éviter les problèmes identifiés par Predictive Insights.
- Si vous vous attendez à voir des anomalies mais qu'aucune n'est affichée, le temps de formation d'Operations Analytics - Predictive Insights est peut-être insuffisant pour produire des anomalies. Deux semaines est le temps de formation standard. Il est également possible qu'une configuration supplémentaire soit nécessaire.

Vues personnalisées

Utilisez la vue Vue universelle d'IBM Cloud Application Business Insights pour améliorer la valeur que les pages du Tableau de bord d'Application Performance prédéfinies fournissent déjà en personnalisant vos propres pages.

La Vue universelle peut servir à afficher les données de surveillance des ressources. Elle ne permet pas d'afficher les données de transaction synthétique, les données de suivi des transactions, les données d'agent de temps de réponse et les données de diagnostic d'analyse approfondie. A l'aide de la Vue universelle, vous pouvez générer rapidement des pages de surveillance pour une application et les sauvegarder à des fins d'affichage. Pendant que vous visualisez une page de tableau de bord personnalisée enregistrée, vous pouvez consulter le tableau de bord en mode actualisation automatique, l'exporter en fichier de données brutes, l'éditer ou le supprimer.

Les quatre rôles par défaut dans Cloud APM, Administrateur de rôles, Administrateur de surveillance, Administrateur système et Utilisateur de surveillance disposent de droits différents concernant l'affichage et la modification des pages de tableau de bord. Pour plus d'informations, voir Tableau 1. Rôles et autorisations .

Les options disponibles dans l'onglet Vues personnalisées varient selon que la page est modifiée ou affichée.

Création et gestion de pages personnalisées

Utilisez l'onglet Vues personnalisées afin de créer ou d'éditer des pages de tableau de bord pour une application, un groupe ou une instance sélectionné en ajoutant ou en mettant à jour des widgets alimentés avec les mesures de ressource de votre choix.

Pourquoi et quand exécuter cette tâche

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Par exemple, l'application Inventory Management dans Cloud APM Démonstration guidée possède les agents de surveillance suivants : Linux OS, MySQL, Node.js, Hadoop et Ruby. Vous pouvez créer et sauvegarder une page personnalisée à n'importe quel niveau du navigateur allant de l'application à l'instance, puis l'ouvrir au niveau où elle a été créée. Une page créée à un niveau particulier ne peut être ouverte qu'au même niveau. Les mesures disponibles pour les widgets peuvent être des ressources, quelles qu'elles soient, de l'application. A l'aide de l'exemple Inventory Management, vous pouvez créer une page avec une table à partir de l'Agent Ruby, un graphique à partir de l'Agent Linux OS, etc.

Procédure

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Pour créer et personnaliser une page de tableau de bord, procédez comme suit :

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, sélectionnez une application. L'onglet Vues personnalisées s'affiche après Présentation du statut et Evénements. Vous pouvez également explorer en aval jusqu'au groupe, sous-groupe ou niveau d'instance du navigateur.
2. Cliquez sur l'onglet **Vues personnalisées**. L'onglet affiche la fenêtre de sélection d'un modèle pour votre page personnalisée ou la page par défaut si cette dernière est déjà définie.
   - Si la fenêtre de sélection d'un modèle pour votre page personnalisée s'ouvre, passez à l'étape 4.
   - Si la page par défaut est affichée, passez à l'étape 3.
3. Cliquez sur **Ajouter** pour créer une page.
4. Cliquez sur un modèle parmi les options de modèle par défaut suivantes :
   - Modèle 1x1
   - Modèle 1x2
   - Modèle 2x2
   - Modèle 2x3
   - Modèle 3x3
   - Modèle 3x2
   - Modèle 2x1
   - Modèle 1x3
   - Modèle 3x1

   Si vous cliquez sur **Précédent**, la page marquée comme favori ou la première page de la liste s'ouvre. S'il n'existe aucune page, la fenêtre de sélection d'un modèle pour votre page personnalisée s'ouvre.
5. Personnalisez le modèle. Pour plus de détails, voir Personnalisation des modèles.
6. Créez un widget. Pour plus de détails, voir «Définition des propriétés de widget», à la page 1164.
7. Cliquez sur **Set Default Timeframe for the page** et définissez la durée de conservation par défaut des données de la page sur 1, 2, 4, 12 ou 24 heures.
8. Lorsque vous êtes prêt à sauvegarder la page, procédez comme suit :
   a. Dans la zone **Nom de page**, entrez un nom de page.

      Important : Les espaces, les traits de soulignement (_) et les tirets (-) sont autorisés dans la zone **Nom de page**. Les tirets suivis d'un trait de soulignement (-_) ne sont toutefois pas autorisés. Par exemple, `System-_Overview` n'est pas autorisé.
   b. Cliquez sur **Sauvegarder**. Les modifications suivantes peuvent être effectuées sur le tableau de bord ou un message peut s'afficher :
      - Le message `Tableau de bord enregistré` est affiché.

- Si * est sélectionné dans **Set Conditions**, le message suivant s'affiche :

  ```
  You selected * in Resource Instance or in Set Conditions, which will result in a large
  number of data series (such as lines on a graph). The large number of data series can
  make the page readability or performance unusable. The advisable limit for this chart
  is 50 data series. Adding specific values helps to narrow the data within recommended
  limits and results in a better user experience.
  ```

- Un indicateur rouge s'affiche sur l'icône  pour indiquer que le type de graphique n'est pas sélectionné et que vous devez le sélectionner.

- Un indicateur rouge s'affiche sur l'icône  pour indiquer que Select Metric n'est pas sélectionné et que vous devez le sélectionner ; le message suivant s'affiche ensuite :

  ```
  A metric must be saved to save a chart.
  ```

9. Sélectionnez l'une des options suivantes dans la barre de titre de la page :

Option	Description

 **Retrieve latest resource Metric Types**	Cliquez sur cette icône pour actualiser les types de mesure. Si le type de mesure ou la mesure a changé lorsqu'un correctif d'agent est appliqué, vous devez actualiser les types de mesure.
	
	L'intervalle entre deux actualisations est limité à 15 minutes. Si vous cliquez sur  **Retrieve latest resource Metric Types** moins de 15 minutes après la dernière actualisation, le message suivant s'affiche :
	`Metadata cache was refreshed recently.`
	`Please wait for` *`time_remaining`* `minute(s) to reload it.`
	
	Lors du chargement des métadonnées, une image de chargement s'affiche.
	
	Lorsque les métadonnées sont chargées, le message suivant s'affiche :
	`Metadata Cache reloaded successfully.`
	
	Si l'actualisation des métadonnées prend plus de 30 secondes, le message suivant s'affiche :
	`Reloading of Metadata cache might take some more time.`
	`Do you want to wait until it is done?`
	
	Vous pouvez cliquer sur **Ok** ou sur **Annuler**.

Option	Description

Afficher le tableau de bord	Cliquez sur cette icône pour afficher les données dans le tableau de bord.
	
	Important : Le nombre limite de lignes renvoyées par définition de données est de 11 000 lignes. Par défaut, les données les plus récentes s'affichent lorsque la limite est dépassée. Pour un volume de données important, les données ne s'affichent pas toutes pour l'intervalle sélectionné. Par exemple, si vous choisissez de visualiser les données de ces dernières 24 heures pour une source de données dont le volume est élevé, seules les données de ces 6 dernières heures peuvent s'afficher si la limite de 11 000 lignes est atteinte.
	
	Si dans un graphique, la série de données dépasse 50, le message suivant s'affiche dans le widget :
	
	`This chart cannot be loaded because the number of data series (such as lines on a graph) exceeds 50. The number of data series is currently` *`current_data_series`*`. You can reduce the number by selecting fewer metrics or resources instances, or by refining the Conditions per Metric. For more information, see Defining widget properties: for Cloud APM - http://ibm.biz/widgetprops and for Cloud APM Private - http://ibm.biz/widgetprops-private`
	
	Si le chargement d'un graphique prend plus de 30 secondes, le message suivant s'affiche dans le widget :
	
	`This chart took too long to load because of a large amount of data, long network latency, or connectivity issue. Reduce the number of Resource Instances or refine the Conditions per Metric to narrow down the data. For more information, see Defining widget properties: for Cloud APM - http://ibm.biz/widgetprops and for Cloud APM Private - http://ibm.biz/widgetprops-private`

Enregistrer sous	Cliquez sur la flèche en regard de l'option **Enregistrer**, puis sur **Enregistrer sous** et spécifiez un nom différent dans la zone **Nom de page** pour sauvegarder la page avec un nom différent. **Important :** Si vous spécifiez un nom de page identique à celui d'une page existante, cette dernière est écrasée.
Supprimer	Cliquez sur cette icône pour supprimer la page actuelle.
Back **Précédent**	Cliquez sur cette icône pour retourner à la page précédente ou à la page favorite.

Que faire ensuite

Affichez les pages personnalisées comme décrit dans la rubrique «Affichage de pages personnalisées», à la page 1167.

Personnalisation des modèles

Vous pouvez personnaliser le modèle en redimensionnant, déplaçant ou ajoutant des marques de réservation de widget en fonction de vos besoins.

Pourquoi et quand exécuter cette tâche

A faire : Vous pouvez personnaliser un modèle existant et l'utiliser. Le modèle personnalisé ne peut toutefois pas être sauvegardé pour être utilisé ultérieurement dans le but de créer des tableaux de bord.

Procédure

1. Dans l'onglet Vues personnalisées, cliquez sur **Editer modèle**.

2. Sélectionnez une marque de réservation de widget. Vous pouvez redimensionner une marque de réservation de widget de tous les côtés et la faire glisser vers un autre emplacement. Si les widgets se chevauchent pendant que vous les redimensionnez ou que vous les faites glisser, le message `Opération de redimensionnement non valide` ou `Opération de déplacement non valide` est affiché.
3. Pour ajouter une marque de réservation pour le widget à un modèle existant, procédez comme suit :
   a. Cliquez sur **Régler la hauteur de page** dans les options de menu, puis indiquez une valeur plus élevée pour le nombre de lignes et cliquez n'importe où en dehors du menu pour augmenter la hauteur de la page.
   b. Indiquez une marque de réservation pour le widget en fonction de vos besoins dans la zone vide de la page en positionnant et en déplaçant le pointeur pour créer une zone.
4. Utilisez les options de menu suivantes pour effectuer différentes opérations sur le modèle :

Option	Description
Annuler	Permet d'annuler la dernière action.
Rétablir	Permet de rétablir la dernière action.
Désélectionner la case sélectionnée	Pour supprimer un widget, sélectionnez-le et cliquez sur l'icône **Désélectionner la case sélectionnée**.
Réinitialiser	Permet de créer un modèle vide. Pour spécifier une marque de réservation de widget sur le modèle vide, placez le pointeur dans la zone Glisser les modèles ici et faites-le glisser pour créer une zone. Vous pouvez créer des marques de réservation de widget de différentes tailles dans la zone Glisser les modèles ici. Les marques de réservation peuvent être déplacées ou redimensionnées, mais elles ne peuvent pas se chevaucher.
Régler la hauteur de page	Permet de définir la hauteur de la page. Vous pouvez spécifier entre 20 et 120 lignes.

5. Cliquez sur  **Editer modèle** pour utiliser le modèle créé.

Que faire ensuite

Créez le widget. Passez à l'étape 6 de la rubrique Création et gestion de pages personnalisées.

Définition des propriétés de widget

Définissez les différentes propriétés des widgets, telles que les mesures et les graphiques pour afficher les données en temps réel dans les widgets.

Procédure

Pour définir les propriétés d'un widget, procédez comme suit :

1. Dans un widget, cliquez sur  afin de sélectionner un type de graphique pour afficher les données.
   - Linéaire
   - A aires
   - A barres
   - Grille

   Important : Pour les graphiques linéaires, à aires et à barres, s'il existe plus de neuf légendes, la couleur du graphique se répète après la neuvième. La couleur du graphique est la même pour la 1ère et la 10ème légende, la 2ème et la 11ème légende, etc.

   Un indicateur vert s'affiche sur l'icône  pour indiquer que le type de graphique est sélectionné.
2. Spécifiez les propriétés de graphique suivantes pour les graphiques linéaires, à aires et à barres :

- Libellé de l'axe des X
- Libellé de l'axe des Y
- Afficher la légende
- Show Interpolation : données collectées à représenter sur le graphique, qui peuvent inclure des valeurs Null. Par conséquent, lorsque le graphique est tracé, sa ligne est déconnectée si elle rencontre une valeur Null et plusieurs lignes déconnectées apparaissent dans le graphique. Si vous sélectionnez l'interpolation, en présence d'une valeur Null, la ligne ne semble pas déconnectée sur le graphique. Au lieu de cela, elle est connectée à la prochaine valeur valide disponible. Dans ce cas, vous obtenez donc une seule ligne de graphique connectée.

  Remarque : Pour APM version 8.1.4.0 IF0005 et les versions ultérieures, les graphiques à courbes et à aires n'affichent plus de lignes déconnectées pour les valeurs null. Par conséquent, la fonction Show Interpolation n'est plus requise et n'est donc plus prise en charge.

Important : La grille ne possède pas de propriétés.

3. Cliquez sur  pour sélectionner le contenu des mesures.

Option	Description
Type de ressource	Dans la liste **Type de ressource**, sélectionnez une ressource. Les ressources disponibles sont associées à l'application. Si une ressource appartenant à l'application n'est pas disponible dans la liste, sa définition de ressource n'a pas été trouvée. La définition de ressource n'a pas été publiée ou le système géré n'est pas connecté au serveur Cloud APM.
Type de mesure	Dans la liste **Type de mesure**, sélectionnez un jeu de données à inclure dans le widget.
Métrique	Dans la liste **Métrique**, sélectionnez un attribut à inclure dans la vue. Les attributs disponibles sont issus du fichier sélectionné. Pour sélectionner des mesures, procédez comme suit : 1. Cliquez sur la liste **Métrique**. Une fenêtre en incrustation, dans laquelle les mesures sont classées par ordre alphabétique croissant, s'ouvre. 2. Sélectionnez un ou plusieurs attributs répertoriés sous Metrics ou cliquez sur **Select All**. **Remarque :** Lorsque vous cliquez sur **Select All**, toutes les mesures de la liste sont sélectionnées. 3. Cliquez sur  pour ajouter les mesures sous la liste **Selected Metrics**. 4. Pour supprimer une mesure sous **Selected Metrics**, cliquez sur  . 5. Cliquez sur la liste **Resource Instance** pour fermer la fenêtre en incrustation. **Important :** Pour les graphiques linéaires, à aires et à barres, la mesure contenant la valeur numérique doit être sélectionnée. Les mesures contenant des valeurs de chaîne ne peuvent pas être affichées dans ces graphiques. **Conseil :** Pour la grille, sélectionnez les mesures en fonction de la sortie qui s'adapte le mieux à votre visibilité sur l'interface utilisateur.
Instance de ressource	Initialement, la sélection est définie sur *, qui extrait les mesures de toutes les instances de la liste. Conservez la valeur par défaut ou sélectionnez l'instance dans la liste. **Important :** Si vous sélectionnez une instance, ce widget ne peut pas être utilisé pour afficher les données d'un autre agent ou d'une autre instance. Il est toutefois judicieux de préciser l'instance afin d'éviter le traitement de gros volumes de données.

Option	Description
Définir une condition pour le groupe de mesures	Si le **type de mesure** sélectionné comporte plusieurs éléments, tels que des UC ou des disques, l'option de **définition de condition pour le groupe de mesures** affiche d'autres éléments que vous pouvez sélectionner à partir de la zone **WHERE**. **Important :** Indiquez des valeurs pour les éléments dans la zone **WHERE**. Evitez d'indiquer * afin de réduire le traitement de gros volumes de données. Par défaut, la condition WHERE affiche les données de ces 4 dernières heures. Cet intervalle de temps peut être redéfini sur une valeur comprise entre 1 et 24 heures par l'administrateur système ; voir «Modification de l'intervalle de temps pour les données de condition WHERE».
Actions	Cliquez sur **Sauvegarder** pour sauvegarder une mesure. Cliquez sur **Editer** pour éditer une mesure. Cliquez sur **Supprimer** pour supprimer une mesure.

4. Pour ajouter une autre mesure, cliquez sur **+ Ajouter une autre mesure**.

   Important : Non applicable à la grille.
5. Fermez la fenêtre Sélectionner des mesures une fois que toutes les mesures ont été ajoutées. Toutes les mesures sont sauvegardées automatiquement une fois que vous avez fermé la fenêtre Sélectionner des mesures.

   Les modifications suivantes peuvent être effectuées sur le tableau de bord ou un message peut s'afficher :
   - Si * est sélectionné dans la liste **Resource Instance** de n'importe quelle mesure, le message suivant s'affiche :

     ```
     You selected * in Resource Instance or in Set Conditions, which will result in a large number of data series (such as lines on a graph). The large number of data series can make the page readability or performance unusable. The advisable limit for this chart is 50 data series. Adding specific values helps to narrow the data within recommended limits and results in a better user experience.
     ```

   - Un indicateur vert s'affiche sur l'icône pour indiquer que les mesures sont correctement sélectionnées pour limiter les données conformément aux valeurs recommandées.
   - Un indicateur orange s'affiche sur l'icône pour indiquer que les mesures ne sont pas correctement sélectionnées pour limiter les données conformément aux valeurs recommandées. Le symbole * est sélectionné dans **Resource Instance** ou **Set Conditions**.
6. Cliquez sur pour entrer le titre du widget. Si le titre du widget n'est pas ajouté, le premier nom de mesure est affecté automatiquement comme titre de widget.

Que faire ensuite

De la même manière, ajoutez des graphiques, des mesures et des titres à tous les widgets, puis passez à l'étape 7 de la rubrique Création et gestion de pages personnalisées.

Modification de l'intervalle de temps pour les données de condition WHERE

L'intervalle de temps peut être redéfini sur une valeur comprise entre 1 et 24 heures par l'administrateur système.

Procédure

Pour modifier l'intervalle de temps, l'administrateur système peut procéder comme suit :

1. Se connecter au serveur APM sur lequel l'édition est déployée.
2. Sur la ligne de commande, exécuter les commandes suivantes :

   ```
   export CLASSPATH=$CLASSPATH:/rép_install/gaian/lib/derbytools.jar:
   export CLASSPATH=$CLASSPATH:/rép_install/gaian/lib/derbyclient.jar:
   export CLASSPATH=$CLASSPATH:/rép_install/gaian/lib/derby.jar:
   java org.apache.derby.tools.ij
   connect 'jdbc:derby://localhost:<port>/gaiandb;user=gaiandb;password=gIan08pW0rd;';
   ```

   Dans ces commandes, *rép_install* correspond au répertoire dans lequel APM a été déployé ; il s'agit de `/opt/ibm` par défaut.

   Dans la commande connect, *port* correspond à la valeur du port sur lequel la base de données est configurée.
3. Une fois la base de données connectée, exécutez la requête suivante pour modifier les valeurs de l'intervalle :

   ```
   UPDATE "OED_TOOL"."PREFERENCETABLE" SET PREFERENCES='-24H' WHERE FIELD='TIMEINTERVAL';
   Commit;
   Exit;
   ```

   La valeur de l'intervalle est exprimée sous la forme `SET PREFERENCES='-24H'`. Elle peut être redéfinie sur une valeur comprise entre 1H et 24H.

Affichage de pages personnalisées

Après avoir créé et sauvegardé des pages de tableau de bord pour une application, un groupe, un sous-groupe ou une instance dans l'onglet Vues personnalisées, vous pouvez les visualiser à tout moment. Certaines des options que vous pouvez sélectionner incluent l'actualisation de la page, la sélection d'intervalles de temps différents, l'édition de la page pour extraire les données de diverses sources et l'exportation du tableau de bord sous forme de fichier de données brutes.

Procédure

Procédez comme suit pour afficher une page sauvegardée dans l'onglet Vues personnalisées du tableau de bord.

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, sélectionnez une application. L'onglet Vues personnalisées s'affiche après Présentation du statut et Evénements. Vous pouvez également explorer en aval jusqu'au groupe, sous-groupe ou niveau d'instance du navigateur.
2. Sélectionnez l'onglet **Vues personnalisées**. L'onglet affiche la fenêtre de sélection d'un modèle pour votre page personnalisée ou la page par défaut si cette dernière est déjà définie.
3. Cliquez sur dans la liste des pages et sélectionnez l'une des pages sauvegardées de la liste. Les pages disponibles ont été sauvegardées par vous ou ont été partagées par un autre utilisateur. Une fois que vous avez sélectionné une page sauvegardée, les échantillons de données historique et actuel sont rapportés dans la page.
4. Sélectionnez l'une des options d'affichage dans la barre de titre de la page :

Option	Description
Actualiser	Indique que l'actualisation automatique est désactivée. Cliquez dessus pour l'activer.

Option	Description
 **Actualiser**	Indique que l'actualisation automatique est activée. Cliquez dessus pour la désactiver. **Important :** Le délai d'actualisation par défaut est 1 minute.
 **Exporter > Données brutes**	Cliquez sur cette icône pour exporter la page au format DAT. Comme plusieurs fichiers DAT sont exportés, ils sont téléchargés sur votre ordinateur au format ZIP. **A faire :** Si le fichier téléchargé est dépourvu d'extension, ajoutez-lui l'extension zip. **Important :** Si le fichier n'est pas téléchargé sur votre ordinateur, vérifiez si l'option Bloquer les fenêtres publicitaires intempestives est activée. Vous pouvez ajouter ce site à votre liste d'exceptions. Procédez à l'extraction du fichier zip téléchargé (les fichiers extraits sont des fichiers en texte clair). Ce fichier contient le nom de la page, la durée, les filtres, la date, l'heure, l'intervalle, le titre du graphique et les données. Le délimiteur de données est la barre verticale. Vous pouvez ouvrir les fichiers DAT à l'aide de l'éditeur approprié ou importer des fichiers dans Excel en indiquant les séparateurs de valeurs appropriés.
 **Exporter > PDF**	Cliquez sur cette icône pour exporter la page au format PDF. Le fichier contient le nom de la page, l'intervalle de temps, les widgets, le nom du créateur et la date de création du rapport.
 **Editer**	Cliquez sur cette icône pour éditer la page actuelle. Vous pouvez modifier les graphiques et les mesures dans les widgets, ajouter de nouveaux widgets, modifier la période par défaut de la page ou modifier le nom de cette dernière.
 **Supprimer**	Cliquez sur cette icône pour supprimer la page actuelle.
 **Ajouter**	Cliquez dessus pour créer une page. Pour personnaliser la page et la sauvegarder, voir «Création et gestion de pages personnalisées», à la page 1160.

5. Sélectionnez l'une des options d'affichage suivantes dans le widget :

Option	Description
Type de graphique	Cliquez sur l'icône **Type de graphique** et sélectionnez une option appropriée dans la liste pour modifier le type de graphique existant. • Pour les graphiques à courbes et à aires, les options **Courbes** et **Aires** sont disponibles. • Pour le graphique à barres, les options **Barres groupées** et **Histogramme groupé** sont disponibles. **Important :** Pour le quadrillage, il n'existe aucune option de type de graphique. Pour les données affichées dans une grille, vous pouvez filtrer les données comme suit : 1. Cliquez sur **Définir un filtre**. La fenêtre Filtrer s'ouvre. 2. Spécifiez des valeurs pour **Colonne**, **Condition** et **Valeur** pour ajouter une règle de filtrage. **Remarque :** Vous pouvez filtrer des valeurs numériques et des valeurs texte en sélectionnant les conditions appropriées. 3. Cliquez sur **Ajouter une règle de filtrage** pour ajouter une autre règle de filtrage. Vous pouvez ajouter plusieurs règles de filtrage. 4. Dans la zone **Correspondance**, sélectionnez **All rules** ou **Any rule** pour filtrer les données. Vous pouvez sélectionner **Respecter la casse** si vous souhaitez effectuer une recherche en fonction de la casse du texte que vous spécifiez dans la zone **Valeur**. 5. Cliquez sur **Filtre** pour filtrer les données affichées dans la grille. 6. Cliquez sur **Effacer le filtre** pour effacer les résultats du filtrage. 7. Cliquez sur **Annuler** pour fermer la fenêtre Filtrer.
Réduire	Cliquez sur cette icône pour réduire le widget.
Développer	Cliquez sur cette icône pour développer le widget.
Agrandir	Cliquez sur cette icône pour agrandir le widget à la taille de la page.
Restaurer	Cliquez sur cette icône pour restaurer la taille d'origine du widget.
Légendes	Le widget contient des cases à cocher pour chaque mesure. Cochez ou décochez des cases pour chaque mesure afin d'afficher les données d'une ou plusieurs mesures.

6. Vous pouvez filtrer les données sur la page à l'aide des listes **Date**, **Heure** et **Intervalle**. Vous pouvez également définir un filtre personnalisé pour que la page affiche les données correspondant à la date et aux intervalles sélectionnés. Pour utiliser un filtre personnalisé, dans la liste **Intervalle**, sélectionnez **Custom**, puis, dans la fenêtre Time Period Selection, sélectionnez la date et l'heure requises.

   Remarque :
   - L'option de filtre personnalisé est disponible à partir d'APM V8.1.4.0 IF0005. Les pages créées à l'aide de versions précédentes de Cloud APM n'affichent pas l'option de filtre personnalisé.
   - Utilisez un filtre personnalisé pour filtrer les données sur un intervalle minimal d'une minute et un intervalle maximal de 24 heures.
   - Lorsque vous appliquez un filtre personnalisé, dans la fenêtre Time Period Selection, si vous cliquez sur **Annuler**, dans la page du tableau de bord, la liste **Intervalle** n'affiche pas l'intervalle que vous avez appliqué précédemment.

- Si vous appliquez un filtre personnalisé sur une page, les données de cette page ne sont pas actualisées automatiquement.

7. Pour définir une page par défaut, cliquez sur dans la liste de pages, puis cliquez sur  **Favoris** en regard du nom de la page à définir comme page par défaut.

Utilitaires de tableau de bord

Utilisez les options disponibles pour gérer l'apparence et le comportement des pages du **Tableau de bord d'Application Performance**.

Copie de l'URL du tableau de bord

Une fois que vous avez accédé à un emplacement dans votre hiérarchie d'applications, l'URL figurant dans la zone d'adresse du navigateur ne change pas pour la nouvelle vue.

Vous pouvez copier l'URL de la page Tableau de bord d'Application Performance que vous affichez. Collez l'URL dans une nouvelle fenêtre de navigateur pour ouvrir la page de tableau de bord ou utilisez l'URL pour accéder au tableau de bord plus tard ou pour le partager avec d'autres utilisateurs.

Procédure

1. Accédez à la page Tableau de bord d'Application Performance que vous voulez mémoriser.
2. Cliquez sur **Actions** > **Copier URL**.
3. Cliquez avec le bouton droit de la souris sur le lien hypertexte **Lien vers la page en cours** et sélectionnez l'option qui permet de copier l'URL.

Que faire ensuite

Conservez une copie de l'URL ou partagez-la avec d'autres utilisateurs dans votre environnement géré. Une fois que vous collez l'URL dans la zone d'adresse de votre navigateur, la page de tableau de bord cible s'ouvre dans la console Cloud APM.

Si vous n'êtes pas connecté au serveur Cloud APM, vous êtes invité à entrer votre ID utilisateur et votre mot de passe avant que la page de tableau de bord cible puisse être affichée. Si la page Mise en route s'ouvre à la place de la page de tableau de bord, appuyez sur F5 ou cliquez sur le bouton de barre d'outils d'actualisation du navigateur. Vous pouvez désactiver la page Mise en route pour des sessions de travail futures en désélectionnant la case à cocher «Afficher cette page Mise en route au démarrage».

Définition d'une trace

Réglez les paramètres de trace de sorte à aider votre administrateur ou le support IBM à diagnostiquer la cause des problèmes liés au Tableau de bord d'Application Performance.

Plusieurs niveaux de trace sont disponibles lorsque vous utilisez le navigateur et l'onglet Présentation des statuts. Vous pouvez instaurer un niveau de trace détaillé au point exact de l'interface utilisateur où vous rencontrez un problème, puis revenir à un niveau de trace plus général une fois que les données de journal nécessaires ont été capturées. Par exemple, si un tableau de bord donné se comporte de manière inattendue, vous pouvez augmenter le niveau de trace avant d'ouvrir le tableau de bord pour consigner l'activité, puis ramener la consignation de trace à son niveau normal.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour définir le niveau de trace lorsque vous souhaitez augmenter ou réduire le volume de consignation de trace.

Procédure

1. Si le Tableau de bord d'Application Performance n'est pas ouvert, sélectionnez l'option **Performance** dans la barre de navigation.
2. Sélectionnez Toutes mes applications ou une application depuis le navigateur ou l'onglet Présentation des statuts.
3. Cliquez sur **Actions** > **Niveau de trace** et sélectionnez l'un des niveaux suivants :
   - **Détaillé** pour que toutes les activités soient consignées. Le niveau de trace détaillé inclut la consignation de trace de niveau Intermédiaire, Faible et Minimal.
   - **Intermédiaire** pour que les modifications de variable soient consignées (par exemple, pour indiquer quels paramètres ont été transmis et quels calculs ont été effectués). Le niveau de trace Intermédiaire comprend les niveaux de consignation de trace Faible et Minimal.
   - **Faible** pour consigner les erreurs et l'activité liée aux variables. Définissez ce niveau de trace si vous rencontrez un problème du type suivant : aucune donnée n'est renvoyée mais le tableau de bord continue de fonctionner. Le niveau de trace Faible comprend le niveau de consignation de trace Minimal.
   - **Minimal** est le niveau par défaut où seules les erreurs irrémédiables sont sauvegardées. Vous pouvez revenir au niveau de trace Minimal après la collecte d'une séquence d'activités spécifique. Quel que soit le niveau de trace défini avant la déconnexion, la trace revient toujours au niveau le plus bas lors de la connexion suivante.
4. Si vous souhaitez envoyer des enregistrements de performance dans un fichier de journalisation commun, sélectionnez **Activer la consignation des statistiques de performance**. Les informations de performance issues de la console sont écrites sur le serveur, où elles peuvent être combinées avec des statistiques de performance de ce dernier afin de fournir le temps de réponse de transaction de bout en bout. Les informations de performance requises incluent l'heure à laquelle une fonction a été démarrée et l'heure à laquelle elle s'est terminée.

Résultats

La trace est ajustée au niveau choisi. Lors de la prochaine connexion, le niveau de trace est défini sur **Minimal** tant que vous ne le modifiez pas.

Pour réduire le trafic de communications au minimum, les messages de journal sont transférés par lots. Un transfert final est réalisé après votre déconnexion, qu'elle soit manuelle ou après un délai d'attente. (Si le navigateur rencontre un problème, aucun journal final n'est envoyé.) Le journal est enregistré sur l'ordinateur serveur sous le nom `itp.log`. Un nouveau fichier `itp.log` est créé chaque fois que le serveur est redémarré.

Si vous définissez **Activer la consignation des statistiques de performance**, des enregistrements similaires à ceux de l'exemple suivant sont sauvegardés dans *rép_install*`/usr/servers/apmui/logs/itp.log` :

```
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366788</millis>
    <sequence>28008</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
    <thread>96</thread>
    <message>BeginTrace:onSelectApp:272wt877d05</message>
</record>
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366809</millis>
    <sequence>28009</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
```

```
    <method>tracing</method>
    <thread>96</thread>
    <message>EndTrace:onSelectApp:272wt877d05</message>
</record>
```

Verrouillage de la console Cloud APM

Vous pouvez verrouiller temporairement votre session de travail sans devoir vous déconnecter de la console Cloud APM.

La fonction de verrouillage de session est indisponible sur l'iPad d'Apple.

Procédure

1. Lorsque vous êtes connecté à la console Cloud APM, cliquez sur *apmadmin* > **Verrouiller la session** où *apmadmin* correspond à votre nom de connexion. L'écran de connexion s'affiche et votre session est verrouillée.
2. Pour déverrouiller votre session, entrez le mot de passe associé à votre ID utilisateur. Votre session de travail reprend.

Tâches associées:

«Ajustement de la valeur de délai de la console», à la page 1115
Le délai d'expiration par défaut du jeton LTPA est de 200 minutes, au-delà duquel vous êtes automatiquement déconnecté. Vous pouvez modifier la valeur de délai afin de répondre à vos besoins professionnels.

Rapports

Les rapports d'historique sont disponibles dans la console Cloud APM pour les données qui sont recueillies par l'Agent de surveillance des temps de réponse, l'Agent WebSphere Applications et l'Agent Synthetic Playback.

Vous pouvez exécuter les rapports depuis le tableau de bord **Toutes mes applications**. A partir de n'importe quelle page de la console Cloud APM, cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**.

Remarque : Lorsque vous exécutez un rapport pour la première fois, vous devez vous connecter à Tivoli Common Reporting en tant qu'utilisateur autorisé à exécuter les rapports Cloud APM. IBM Cognos Viewer est le visualiseur de sortie de rapport par défaut.

Rapports de l'Agent de surveillance des temps de réponse

Pour afficher les rapports **Performances des applications et utilisation** ou **Comparer les performances des applications sur deux périodes**, sélectionnez une application qui inclut les systèmes gérés par l'Agent de surveillance des temps de réponse, puis sélectionnez **Actions** > **Rapports de lancement**.

Pour afficher le rapport **Toutes mes applications** ou **Comparer les performances de plusieurs applications**, sélectionnez **Toutes mes applications**, puis **Actions** > **Rapports de lancement**.

Rapports de l'Agent WebSphere Applications

Pour afficher n'importe quel rapport de l'Agent WebSphere Applications, sélectionnez une application qui inclut les systèmes gérés par l'Agent WebSphere Applications, puis sélectionnez **Actions** > **Rapports de lancement**.

Agent Synthetic Playback

Pour afficher n'importe quel rapport de l'Agent Synthetic Playback, sélectionnez une application qui inclut les transactions synthétiques, puis **Actions** > **Rapports de lancement**.

Remarque : Si l'option **Rapports de lancement** ne se trouve pas dans le menu **Actions**, vérifiez que les rapports Cloud APM sont correctement installés. Pour plus d'informations, voir «Intégration à Tivoli Common Reporting», à la page 917.

Important : Si les heures correctes des instances de transaction ne s'affichent pas dans les rapports, vous devrez peut-être réinitialiser le fuseau horaire de l'utilisateur dans la zone de connexion Cognos. Pour plus d'informations, voir la note technique sur la conversion du temps en heure locale en fonction du paramètre de fuseau horaire.

Pour plus d'informations sur les navigateurs pris en charge pour visualiser les rapports de l'Agent Synthetic Playback, l'Agent de surveillance des temps de réponse et l'Agent WebSphere Applications, voir les Rapports de compatibilité des produits logiciels pour Cognos 10.2.1.7.

Rapports de l'Agent de surveillance des temps de réponse

Les rapports d'historique sont disponibles pour les données collectées par l'Agent de surveillance des temps de réponse. Les rapports de l'Agent de surveillance des temps de réponse sont indisponibles dans Cloud APM, Base. Ils sont uniquement disponibles dans Cloud APM, Advanced.

Deux types de rapport associés aux données collectées par l'Agent de surveillance des temps de réponse sont disponibles, à savoir les rapports actifs et les rapports simples.

Rapports actifs
Ils s'affichent dans un navigateur au format MHTML. Internet Explorer prend en charge MHTML par défaut. Pour les autres navigateurs, un plug-in de prise en charge de MHTML peut être installé. Les rapports actifs sont également appelés rapports interactifs hors ligne.

Rapports simples
Les rapports simples s'affichent dans IBM Cognos Viewer. Ce dernier est le visualiseur de sortie de rapports par défaut.

Les rapports d'historique prédéfinis suivants associés aux données collectées par l'Agent de surveillance des temps de réponse sont disponibles :

Tableau 225. Rapports d'historique prédéfinis

Rapport	Type
Toutes mes applications	Rapports actifs
Performances des applications et utilisation	Rapports actifs
Comparer les performances des applications sur deux périodes	Simple
Comparer les performances de plusieurs applications	Simple

Pour plus d'informations sur le mappage entre les rapports de l'Agent de surveillance des temps de réponse et de Performance Management, voir Mappages des attributs de l'agent de surveillance des temps de réponse.

Rapport Toutes mes applications

Utilisez le rapport Toutes mes applications pour afficher des informations sur les unités utilisateur, le volume de données, le temps de réponse et le nombre d'erreurs.

Dans ce rapport, vous affichez des informations pour toutes les applications. Spécifiez la période du rapport **Dernier jour** (par défaut), **Semaine dernière** ou **Mois dernier**. Affichez les informations suivantes en fonction de la période sélectionnée par application :

- Graphique à colonnes empilées représentant le nombre de transactions
- Graphique à colonnes représentant le volume des données de transaction

- Graphique à colonnes représentant le temps de réponse moyen des transactions
- Graphique à colonnes empilées représentant les nombres d'erreurs

Rapport Performances des applications et utilisation

Utilisez ce rapport afin d'afficher des informations sur les performances, la disponibilité et les unités utilisateur pour des applications uniques.

Dans la fenêtre **Sélection d'une application**, sélectionnez une application. Cliquez sur **Suivant**. Dans la fenêtre de **sélection des transactions clés pour l'application**, sélectionnez les transactions en fonction desquelles vous voulez filtrer le rapport. Cliquez sur **OK**. Ce rapport se compose de trois onglets : Performances, Disponibilité et Unités. L'intervalle par défaut est semaine.

Dans l'onglet Performances, affichez les informations suivantes en fonction de l'intervalle de temps sélectionné pour l'application que vous consultez actuellement dans le tableau de bord d'Application Performance :

- Graphique à courbes représentant le temps de réponse moyen par transactions (clés)
- Graphique à courbes représentant le temps de réponse moyen des transactions par réussite, erreur de serveur et erreur de client.
- Graphique à courbes et à barres représentant le volume des données de transaction. Les barres représentent le volume des données de transaction et la courbe représente la moyenne du volume de données de transaction.
- Graphique à courbes et à barres représentant le nombre de transactions. Les barres représentent le nombre de transactions et la courbe représente les valeurs polynomiales et la moyenne mobile.

Dans l'onglet Disponibilité, affichez les informations suivantes en fonction de l'intervalle de temps sélectionné pour l'application que vous consultez actuellement dans le tableau de bord d'Application Performance :

- Graphique à barres empilées représentant le pourcentage des transactions réussies et le pourcentage des transactions ayant échoué ; les échecs sont répartis en deux catégories, les erreurs de serveur et les erreurs de client.
- Graphique à barres empilées représentant le nombre de transactions réussies et le nombre de transactions ayant échoué ; les échecs sont répartis en deux catégories, les erreurs de serveur et les erreurs de client.
- Graphique circulaire représentant les codes d'erreur les plus fréquents

Dans l'onglet Unités, affichez les informations suivantes en fonction de l'intervalle de temps sélectionné pour l'application que vous consultez actuellement dans le tableau de bord d'Application Performance :

- Graphique à barres représentant les transactions par type d'unité
- Graphique à barres représentant les transactions par système d'exploitation d'unité
- Graphique à barres représentant les transactions par navigateur d'unité
- Tableau représentant les performances des transactions par dimensions. Vous pouvez filtrer ce tableau par type d'unité, système d'exploitation d'unité, marque d'unité et navigateur d'unité.

Rapport Comparer les performances des applications sur deux périodes

Utilisez ce rapport pour examiner les performances d'une application sélectionnée.

Dans la fenêtre **Sélection de l'application et de la fréquence**, spécifiez une application et une fréquence (hebdomadaire, quotidienne, mensuelle). Dans la fenêtre **Sélection des périodes**, choisissez les périodes appropriées pour l'intervalle et cliquez sur **OK**.

Le rapport affiche les graphiques suivants pour l'application sélectionnée, pour les périodes sélectionnées, par intervalle de temps sélectionné :

- Graphique à courbes représentant le nombre de transactions pour le type d'unité

- Graphique à courbes représentant le volume des transactions
- Graphique à courbes représentant le temps de réponse moyen
- Graphique à courbes représentant le nombre d'erreurs

Rapport Comparer les performances de plusieurs applications

Utilisez ce rapport pour comparer les performances de plusieurs applications pour la même période de temps.

Dans la fenêtre **Sélection de l'application et de la fréquence**, spécifiez une application et une fréquence (hebdomadaire, quotidienne, mensuelle). Cliquez sur **Suivant**. Choisissez une période appropriée pour l'intervalle.

Le rapport affiche les graphiques suivants pour les applications sélectionnées, pour les périodes sélectionnées, par intervalle de temps sélectionné :

- Graphique à courbes représentant le nombre de transactions
- Graphique à courbes représentant le volume des données de transaction
- Graphique à courbes représentant le temps de réponse moyen
- Graphique à courbes représentant le nombre d'erreurs

Mappage des attributs de l'Agent de surveillance des temps de réponse

Certains rapports Cloud APM se basent sur les données collectées par l'Agent de surveillance des temps de réponse. Les données contenues dans ces rapports sont mappées aux attributs de l'Agent de surveillance des temps de réponse.

Le tableau suivant décrit le mappage des éléments de données dans les rapports de l'Agent de surveillance des temps de réponse aux attributs de l'agent :

Tableau 226. Mappage des attributs de l'Agent de surveillance des temps de réponse

Elément de données du rapport	Description	Nom de l'attribut ODI	Colonne du fichier ODI
Nom de l'application	Nom de l'application surveillée signalé à la console Cloud APM	Nom de l'application	T5TXCS.APPLICATIN
Nombre de transactions	Nombre total de séquences de demandes et de réponses qui sont observées par l'agent de surveillance au cours de l'intervalle d'agrégat.	Nombre total de requêtes	T5TXINS.TOTREQ
Erreurs client	Nombre de requêtes HTTP ayant le code d'état 400 - 499.	Erreurs client	T5TXCS.NUM4XX
Erreurs de serveur	Nombre de requêtes HTTP ayant le code d'état 500 - 599.	Erreurs de serveur	T5TXCS.NUM5XX
Nom de transaction	Nom de transaction signalé à Application Management Console.	Nom de transaction	T5TXCS.TRANSACTN
Statut de la transaction	Code de réponse associé à la transaction.	Code de statut	T5TXCS.STATUSCODE

Tableau 226. Mappage des attributs de l'Agent de surveillance des temps de réponse (suite)

Elément de données du rapport	Description	Nom de l'attribut ODI	Colonne du fichier ODI
Nombre de kilooctets de réponse du code	Nombre total de kilooctets dans chaque réponse de la demande au cours de l'intervalle de données.	Octets de réponse	T5TXCS.REPLYBYT
Nombre de kilooctets de demande	Nombre total de kilooctets dans la demande au cours de l'intervalle de données.	Demande ko	T5TXCS.REQBYTES
Nombre total de kilooctets	Nombre total de kilooctets transférés pour toutes les demandes au cours de la période.	Total des octets	T5TXCS.TOTBYTES
Nombre total d'objets	Nombre total d'objets imbriqués dans une page Web au cours de la période	Nombre total d'objets	T5TXCS.OBJCNT
Taille totale des objets	Taille totale de tous les objets imbriqués dans la page Web au cours de la période.	Taille totale des objets	T5TXCS.OBJSIZE
Temps de réponse (en secondes)	Nombre total de secondes nécessaires à l'exécution de la transaction serveur.	Temps de réponse	T5TXCS.RESPTIME
Temps de rendu	Délai exprimé en secondes nécessaire au rendu complet de la page Web dans le navigateur en utilisant des balises JavaScript intégrées.	Temps de rendu	T5TXCS.RENDERTIME
Temps client	Délai d'exécution moyen exprimé en secondes d'une transaction sur le client au cours de la période de surveillance en cours.	Délai client moyen	T5TXCS.CLIENTTIME
Temps de chargement	Temps moyen, en secondes, qui s'est écoulé depuis la demande de téléchargement d'un utilisateur jusqu'à la fin du téléchargement de l'objet Web.	Temps de chargement moyen	T5TXCS.LOADTIME
Navigateur	Description du navigateur Web dans lequel la page Web s'affiche.	Description du navigateur	T5TXCS.BROWSEDESC
Serveur	Nom ou adresse IP du serveur pour la Transaction TCP.	Description du serveur	T5TXCS.SERVERDESC
Nom d'hôte d'URL	Nom d'hôte TCP/IP de l'URL.	Nom d'hôte d'URL	T5TXCS.URLHOST
URL de la méthode	Méthode utilisée pour exécuter des requêtes HTTP (GET, POST, HEAD, PUT, OPTIONS, DELETE, TRACE ou CONNECT).	Méthode	T5TXCS.METHOD

Tableau 226. Mappage des attributs de l'Agent de surveillance des temps de réponse (suite)

Elément de données du rapport	Description	Nom de l'attribut ODI	Colonne du fichier ODI
Détails de l'adresse URL	Chemin d'URL du fichier sur le serveur hébergeant la page Web.	Chemin de l'adresse URL	T5TXCS.URLPATH

Pour plus d'informations sur l'Agent de surveillance des temps de réponse, voir Transaction Monitoring Reference.

Génération de rapports sur l'Agent Synthetic Playback

Exécutez des rapports pour les applications associées à des transactions synthétiques.

Pourquoi et quand exécuter cette tâche

Sélectionnez une application et une transaction synthétique associée dans le Tableau de bord d'Application Performance, puis générez des rapports reposant sur votre sélection.

Cinq rapports de plusieurs pages sont disponibles :

Vue globale des transactions

Ce rapport de deux pages affiche les temps de réponse et les facteurs de disponibilité de la transaction synthétique sélectionnée sur une plage de dates définie.

La première page affiche les données suivantes :

- Un graphique à courbes des temps de réponse des transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant les temps de réponse moyens, en secondes, de chaque transaction synthétique sur la plage de dates définie

La deuxième page affiche les données suivantes :

- Un graphique à courbes des facteurs de disponibilité des transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant le facteur de disponibilité moyen de chaque transaction synthétique sur la plage de dates définie

Vous avez accès à deux rapports supplémentaires à partir du rapport Vue globale des transactions : Timely Analysis by Transactions et HTTP Metrics by Transactions.

Timely Analysis by Transaction affiche les indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée sur la plage de dates définie

HTTP Metrics by Transaction affiche les indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée sur la plage de dates définie

Transaction Detail By Locations

Ce rapport de deux pages affiche les temps de réponse et les facteurs de disponibilité par emplacement des transactions et des sous-transactions synthétiques sélectionnées sur une plage de dates définie.

La première page affiche les données suivantes :

- Des graphiques à courbes retraçant les temps de réponse, par emplacement, des transactions et sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Des tableaux répertoriant les temps de réponse moyens, en secondes, de toutes les sous-transactions synthétiques sur une plage de dates définie, sur chaque emplacement

La deuxième page affiche les données suivantes :

- Des graphiques à courbes des facteurs de disponibilité, par emplacement, des transactions et sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Des tableaux répertoriant les facteurs de disponibilité moyens de toutes les sous-transactions synthétiques sur une plage de dates définie, sur chaque emplacement

Vous pouvez accéder à quatre rapports supplémentaires à partir du rapport Détails de transaction par emplacements : Timely Analysis by Locations of Transaction, HTTP Metrics by Locations of Transaction, Timely Analysis by Locations of Subtransaction et HTTP Metrics by Locations of Subtransaction.

Timely Analysis by Locations of Transaction affiche les indicateurs HTTP d'une transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée par emplacements sur la plage de dates définie

HTTP Metrics by Locations of Transaction affiche les indicateurs HTTP d'une transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée par emplacements sur la plage de dates définie

Timely Analysis by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée par emplacements sur la plage de dates définie

HTTP Metrics by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée par emplacements sur la plage de dates définie

Transaction Detail By Subtransactions

Ce rapport de deux pages affiche les temps de réponse et les facteurs de disponibilité des sous-transactions à des intervalles définis, sur une plage de dates définie.

La première page affiche les données suivantes :

- Un graphique à courbes retraçant les temps de réponse des sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant les temps de réponse moyens, en secondes, de chaque sous-transaction synthétique sur la plage de dates définie

La deuxième page affiche les données suivantes :

- Un graphique à courbes des facteurs de disponibilité des sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant les facteurs de disponibilité de chaque sous-transaction synthétique sur la plage de dates définie

Vous avez accès à deux rapports supplémentaires à partir du rapport Détails de transaction par sous-transactions : Timely Analysis by Subtransactions et HTTP Metrics by Subtransactions.

Timely Analysis by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée à des intervalles définis sur une plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée sur la plage de dates définie

HTTP Metrics by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée à des intervalles définis sur une plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée sur la plage de dates définie

Tendance des transactions

Ce rapport de quatre pages affiche une analyse des tendances des temps de réponse, des facteurs de disponibilité et des indicateurs HTTP au cours de la semaine précédente et des cinq semaines précédentes.

La première page affiche les données de tendance pour les temps de réponse et les facteurs de disponibilité d'une transaction synthétique :

- Un graphique à courbes combiné des temps de réponse moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes
- Un graphique à courbes combiné du facteur de disponibilité d'une transaction synthétique sélectionnée qui compare le facteur de disponibilité pour la semaine précédente au facteur de disponibilité de référence au cours des 5 semaines précédentes
- Un tableau du temps de réponse moyen et du facteur de disponibilité d'une transaction synthétique au cours de la semaine précédente et au cours de la plage de dates des cinq semaines précédentes
- Un graphique à courbes combiné des temps de réponse moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes, par emplacement
- Un graphique à courbes combiné du facteur de disponibilité d'une transaction synthétique sélectionnée qui compare le facteur de disponibilité pour la semaine précédente au facteur de disponibilité de référence de base au cours des 5 semaines précédentes, par emplacement

- Un tableau des temps de réponse moyens et des facteurs de disponibilité d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes, par emplacement
- Un graphique à courbes combiné des temps de réponse moyens des sous-transactions d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes
- Un graphique à courbes combiné des facteurs de disponibilité moyens des sous-transactions d'une transaction synthétique sélectionnée qui compare le facteur de disponibilité pour la semaine précédente au facteur de disponibilité de référence au cours des 5 semaines précédentes
- Un tableau des temps de réponse moyens et des facteurs de disponibilité des sous-transactions d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes

La deuxième page affiche des données de tendance pour les mesures HTTP d'une transaction synthétique :

- Un graphique à courbes combiné des temps de blocage moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps DNS moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps SSL moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps de connexion moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps d'envoi moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps de réception moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps de rendu moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un tableau des indicateurs HTTP moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes

La troisième page affiche des données de tendance relatives aux indicateurs HTTP, en millisecondes, d'une transaction synthétique par emplacement. Les graphiques et le tableau comparent les moyennes des indicateurs HTTP au cours de la semaine précédente avec la moyenne des mesures de référence au cours des 5 semaines précédentes :

- Sept graphiques à courbes combinés qui comparent les valeurs moyennes de différents indicateurs HTTP d'une transaction synthétique sélectionnée pour la semaine précédente avec l'indicateur de référence au cours des 5 semaines précédentes par emplacement
- Un tableau des valeurs moyennes des indicateurs HTTP d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes

La quatrième page affiche des données de tendance relatives aux indicateurs HTTP, en millisecondes, pour des sous-transactions. Les graphiques et le tableau comparent les moyennes des indicateurs HTTP au cours de la semaine précédente avec les moyennes des mesures de référence au cours des 5 semaines précédentes :

- Sept graphiques à courbes combinés qui comparent les valeurs moyennes de différents indicateurs HTTP d'une transaction synthétique sélectionnée pour la semaine précédente avec l'indicateur de référence au cours des 5 semaines précédentes par sous-transaction
- Un tableau des valeurs moyennes des indicateurs HTTP d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes par sous-transaction

Tendance des sous-transactions

Ce rapport de deux pages affiche une analyse des tendances des temps de réponse, des facteurs de disponibilité et des indicateurs HTTP pour des sous-transactions au cours de la semaine précédente et des 5 semaines précédentes.

La première page affiche les données de tendance pour les temps de réponse et les facteurs de disponibilité de sous-transactions pour le dimanche précédent, la semaine précédente et les 5 semaines précédentes :

- Un tableau qui compare les données de tendance pour les temps de réponse et les facteurs de disponibilité de sous-transactions pour le dimanche précédent, la semaine précédente et les 5 semaines précédentes
- Un graphique à courbes combiné qui compare les temps de réponse moyens de sous-transactions au cours de la semaine précédente avec le temps de réponse de référence au cours des 5 semaines précédentes
- Un graphique à courbes combiné qui compare les fréquences de disponibilité moyennes de sous-transactions au cours de la semaine précédente avec la fréquence de disponibilité de référence au cours des 5 semaines précédentes
- Un tableau des temps de réponse moyens et des fréquences de disponibilité moyennes de sous-transactions pour la semaine précédente.
- Un tableau des temps de réponse moyens et des fréquences de disponibilité moyennes de sous-transactions pour les 5 semaines précédentes.

La deuxième page affiche des données de tendance relatives aux indicateurs HTTP, en millisecondes, pour des sous-transactions. Les graphiques et les tableaux comparent les moyennes des indicateurs HTTP des sous-transactions au cours de la semaine précédente avec les moyennes des mesures de référence au cours des 5 semaines précédentes :

- Sept tableaux contenant les valeurs moyennes des indicateurs HTTP de la transaction sélectionnée pour le dimanche précédent, la semaine précédente et au cours des 5 semaines précédentes par sous-transactions
- Sept graphiques à courbes combinés qui comparent les valeurs moyennes de différents indicateurs HTTP en millisecondes de la transaction sélectionnée pour la semaine précédente avec le rapport de disponibilité de référence au cours des 5 semaines précédentes par sous-transactions
- Un tableau des valeurs moyennes des indicateurs HTTP des sous-transactions pour la semaine précédente.
- Un tableau des valeurs moyennes des indicateurs HTTP des sous-transactions pour les 5 semaines précédentes.

Procédure

Pour générer des rapports, procédez comme suit :

1. Cliquez sur l'icône **Performance** et sélectionnez **Tableau de bord d'Application Performance**. Pour sélectionner une application, développez **Toutes mes applications**, puis sélectionnez une application. Pour afficher toutes les transactions synthétiques associées à l'application sélectionnée, cliquez sur **Groupes** > **Transactions** > **Transactions synthétiques**.
2. Sélectionnez une transaction synthétique dans le tableau Liste des transactions. Pour exécuter un rapport, cliquez sur **Actions** > **Rapports de lancement** et sélectionnez l'un des rapports suivants :
   - **Vue globale des transactions**
   - **Transaction Detail By Locations**
   - **Transaction Detail By Subtransactions**
   - **Tendance des transactions**
   - **Tendance des sous-transactions**

Une page de configuration s'ouvre dans un nouvel onglet de votre navigateur Web.

3. Pour définir une plage de dates pour votre rapport, sélectionnez une plage de dates prédéfinie ou entrez une plage de dates personnalisée.
4. Pour définir un intervalle de temps pour votre rapport, sélectionnez un intervalle dans **Time Type**. Configurez votre rapport pour qu'il affiche des données à partir de vos transactions et sous-transactions synthétiques à intervalles **horaires**, **journaliers** ou **hebdomadaires**, sur la plage de dates définie. Pour générer votre rapport, cliquez sur **Terminer**.
5. Pour visualiser les rapports sur les indicateurs HTTP pour les transactions, les sous-transactions ou les emplacements, vous devez sélectionner une transaction, une sous-transaction ou un emplacement dans les rapports **Vue globale des transactions**, **Détails de transaction par emplacements** ou **Détails de transaction par sous-transactions**.
   - Pour visualiser le rapport Timely Analysis by Transactions, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Vue globale des transactions** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport HTTP Metrics by Transactions, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Vue globale des transactions** et sélectionnez **Go To** > **Http Metrics Aggregation**.
   - Pour visualiser le rapport Timely Analysis by Locations of Transaction, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Détails de transaction par emplacements** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport HTTP Metrics by Locations of Transaction, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Détails de transaction par emplacements** et sélectionnez **Go To** > **Http Metrics Aggregation**.
   - Pour visualiser le rapport Timely Analysis by Locations of Subtransaction, cliquez avec le bouton droit de la souris sur un nom de sous transaction dans le rapport **Détails de transaction par emplacement** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport HTTP Metrics by Locations of Subtransaction, cliquez avec le bouton droit de la souris sur un nom de sous transaction dans le rapport **Détails de transaction par emplacement** et sélectionnez **Go To** > **Http Metrics Aggregation**.
   - Pour visualiser le rapport Timely Analysis by Subtransactions, cliquez avec le bouton droit de la souris sur un nom de sous-transaction dans le rapport **Tendance des sous-transactions** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport HTTP Metrics by Subtransactions, cliquez avec le bouton droit de la souris sur un nom de sous-transaction dans le rapport **Tendance des sous-transactions** et sélectionnez **Go To** > **Http Metrics Aggregation**.

Rapports de l'Agent WebSphere Applications

Les rapports prédéfinis sont disponibles pour les données collectées par l'Agent WebSphere Applications.

Les rapports suivants associés aux données collectées par l'Agent WebSphere Applications sont disponibles :

Performances des demandes d'application

Description

Ce rapport analyse la manière dont les applications sont exécutées à un niveau d'agrégation sur un serveur d'applications. Le graphique circulaire illustre les demandes de niveau d'agrégation des applications. Le graphique à barres représente le temps de réponse moyen des applications à un niveau d'agrégation. Les deux graphiques en lignes de série temporelle affichent le temps de réponse moyen et la tendance du nombre total de demandes pour toutes les applications. Pour explorer les demandes individuelles d'une application, cliquez sur un secteur de graphique ou une barre.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement et Type de serveur d'applications

Tables utilisées

Request_Analysis_*V

Pools de connexions de base de données

Description

Ce rapport analyse les pools de connexions à la base de données dans un serveur d'applications. Le tableau contient des statistiques clés pour tous les pools de connexions à un niveau d'agrégation. Lorsque vous sélectionnez une source de données spécifique, deux graphiques de tendance indiquent la tendance des statistiques clés.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du serveur d'applications

Tables utilisées

DB_Connection_Pools_*V

Performances EJB

Description

Ce rapport analyse la façon dont les EJB déployés dans le serveur d'applications s'exécutent. Le graphique circulaire illustre le nombre de méthodes au niveau d'agrégation pour les EJB. Le graphique à barres représente le temps de réponse moyen des méthodes dans les EJB à un niveau d'agrégation. Les deux graphiques de série temporelle illustrent une tendance de nombre d'appels de méthode et une tendance de temps de réponse moyen de méthode pour tous les EJB. Les lignes de tendance peuvent être filtrées par EJB via un clic sur une ligne de la liste.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du serveur d'applications

Tables utilisées

Enterprise_Java_Beans_*V

Utilisation de la récupération de place du serveur d'applications

Description

Ce rapport analyse la récupération de place. Utilisez-le pour déterminer si la récupération de place est source de problèmes ou si la taille du segment de mémoire est incorrecte. Le premier graphique illustre le pourcentage de segment de mémoire moyen utilisé et le pourcentage de récupération de place moyen en temps réel dans le temps. Le deuxième graphique illustre le pourcentage d'exécution de la récupération de place moyen en temps réel et le taux de récupération de place moyen.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Garbage_Collection_Analysis_*V

Utilisation de la JVM pour le serveur d'applications

Description

Ce rapport analyse la manière dont la JVM d'un serveur d'applications s'exécute. Le graphique à barres empilées indique la manière dont la mémoire JVM est utilisée et libérée. Le graphique à double courbe indique la consommation d'UC de la JVM au regard de l'utilisation de la mémoire JVM.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Application_Server_*V

Pools d'unités d'exécution

Description

Ce rapport analyse les pools d'unités d'exécution dans un serveur d'applications. Le tableau contient des statistiques clés pour tous les pools d'unités d'exécution à un niveau d'agrégation. Une fois qu'un pool d'unités d'exécution est sélectionné dans la liste, le diagramme de tendances indique la tendance des statistiques clés pour le pool d'unités d'exécution sélectionné. Si aucun pool d'unités d'exécution n'est sélectionné, les tendances indiquent un récapitulatif de tous les pools d'unités d'exécution.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Thread_Pools_*V

Performances des applications Web

Description

Ce rapport analyse la manière dont les applications s'exécutent dans le conteneur Web d'un serveur d'applications (données PMI). Le graphique circulaire illustre les demandes de niveau d'agrégation des applications. Le graphique à barres représente le temps de réponse moyen des applications à un niveau d'agrégation. Les deux graphiques en lignes de série temporelle affichent le temps de réponse moyen et la tendance du nombre total de demandes pour toutes les applications. Cliquez sur un secteur de graphique, une barre ou une ligne pour explorer le(s) servlet(s)/page(s) jsp d'une application.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Thread_Pools_*V

Performances des demandes d'application pour les clusters

Description

Ce rapport analyse la manière dont les serveurs s'exécutent dans un cluster. Le premier graphique illustre le nombre de demandes effectuées par chacun des membres du cluster au cours de l'intervalle de temps sélectionné. Le deuxième graphique fournit des informations sur la

tendance de temps de réponse moyen pour chaque membre du cluster. Le graphique contient une ligne distincte pour chaque serveur du cluster. Cliquez sur une ligne pour explorer les données du serveur individuel. Le rapport Performances des demandes d'application associé à ce serveur s'ouvre.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du cluster

Tables utilisées

Request_Analysis_*V

Utilisation de la JVM et de la récupération de place pour les clusters

Description

Ce rapport analyse la JVM et les tendances d'utilisation de la récupération de place par chacun des membres du cluster. Le premier graphique illustre le pourcentage d'exécution de la récupération de place moyen en temps réel. Le deuxième graphique illustre le pourcentage de segment de mémoire moyen utilisé. Les derniers graphiques illustrent l'utilisation de la mémoire de l'unité centrale et de la JVM. Tous ces graphiques illustrent des données relatives à chaque membre du cluster sur une ligne distincte.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du cluster

Tables utilisées

Garbage_Collection_Analysis_*V, Application_server_*V

Applications principales avec les temps de réponse les plus lents sur l'ensemble des serveurs

Description

Ce rapport analyse la manière dont les applications sont exécutées à un niveau d'agrégation sur tous les serveurs d'applications. Un graphique à barres représente le temps de réponse moyen des applications à un niveau d'agrégation.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nombre d'applications

Chapitre 15. IBM Cloud Application Business Insights

Utilisez l'application Cloud Application Business Insights pour créer et afficher des tableaux de bord personnalisés offrant une présentation détaillée des performances de toutes vos applications. Vous pouvez créer des représentations visuelles complexes, dynamiques et interactives à partir de sources de données Cloud APM et Tivoli Monitoring pour afficher des données en temps réel. Vous pouvez également vous connecter à d'autres sources de données tierces.

Composants de Cloud Application Business Insights

Il comprend les composants suivants :

Dashboard Designer

Composant de générateur de tableau de bord. Outil Web dotée d'une interface intuitive de type glisser-déposer qui permet de créer et partager des tableaux de bord opérationnels offrant des données en temps réel. Vous pouvez masquer les données critiques d'entreprise dans des tableaux de bord interactifs, puis les personnaliser.

Moteur

Composant de visualisation des données. Le moteur est déployé en tant qu'application Web sur WebSphere Application Server Liberty.

Connecteur

Composant de requête de données qui se connecte à une source de données et extrait des données pour les représentations visuelles dans les widgets. Par défaut, Cloud Application Business Insights dispose de connecteurs pour les sources de données Cloud APM et Tivoli Monitoring.

Vous pouvez également vous connecter à des sources de données tierces à l'aide des pilotes JDBC de la plupart des bases de données relationnelles.

Plus d'informations

Pour plus d'informations sur l'installation, l'administration et l'utilisation de l'application, voir les liens suivants :

- Présentation de Cloud Application Business Insights
- Installation de Cloud Application Business Insights
- Administration de Cloud Application Business Insights
- Utilisation de Cloud Application Business Insights

© Copyright IBM Corp. 2015, 2018

Chapitre 16. Traitement des incidents et support

Consultez les entrées sur le traitement des incidents que vous pouvez rencontrer lors de l'installation, la configuration ou l'utilisation de IBM Cloud Application Performance Management.

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management sur le site developerWorks. Vous pouvez rechercher les entrées qui commencent par «Traitement des incidents», répondre à une entrée pour poser une question associée ou créer une entrée contenant votre question.

Des fonctions supplémentaires et des informations sur l'identification et la résolution des problèmes spécifiques à l'agent sont disponibles :

- Pour la Passerelle hybride d'IBM Cloud Application Performance Management, voir «Gestion de la passerelle hybride», à la page 886

Collecte des journaux du serveur Cloud APM pour le support IBM

Collectez les fichiers journaux du serveur Cloud APM et les composants de prise en charge à la demande du support IBM en vue du diagnostic des problèmes.

Avant de commencer

L'autorisation racine est requise pour collecter les informations système du serveur Cloud APM.

Important : Les fichiers journaux du serveur Cloud APM commencent à boucler lorsqu'ils atteignent le nombre et la taille définis. L'espace disque requis pour le serveur Cloud APM prend en compte le nombre et la taille des fichiers journaux configurés par défaut. Il est recommandé d'utiliser un agent OS pour surveiller l'utilisation de l'espace disque sur le serveur Cloud APM.

Procédure

Pour exécuter la commande de collecte de journaux, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire `/opt/ibm/ccm/` de l' du serveur Cloud APM ou au répertoire que vous avez spécifié lorsque vous avez installé le serveur.
2. Exécutez la commande suivante :
   ```
   ./collectLogs.sh
   ```
   Un fichier `tar.gz` dont le nom comporte un horodatage est généré dans le répertoire `/tmp`. Par exemple, `/tmp/SCMAI_Logs_`*`nom_hôte_min`*`_20150207_105132.tar.gz`.
   Il se peut que vous receviez un message indiquant que le système ne parvient pas à trouver le chemin spécifié. Vous pouvez ignorer ce message.
3. Envoyez le fichier de sortie à votre interlocuteur du support IBM.

Résultats

Le script regroupe les journaux des composants suivants. Les chemins d'accès au répertoire des journaux répertoriés dans le tableau ci-dessous commencent par le répertoire d'installation `/opt/ibm` par défaut. Si vous avez spécifié un répertoire d'installation différent lors de l'installation du serveur, vos chemins d'accès au répertoire des journaux incluent ce répertoire d'installation.

© Copyright IBM Corp. 2015, 2018

Tableau 227. Fichiers journaux collectés par le script collectLogs.sh.

Composant	Répertoire du journal	Nom du fichier journal	Description
serveur Cloud APM	/opt/ibm/wlp/usr/servers/min/logs	messages.log	Fichier journal principal du serveur Cloud APM.
		Fichier journal principal de l'interface de l'agent :server.xml, jvm.options, bootstrap.properties	Informations sur la configuration et la machine virtuelle Java de l'interface de l'agent.
		Fichiers journaux de l'interface de l'agent : messages.log, console.log,trace.log	Traces et messages standard de l'interface de l'agent.
		Outil de diagnostic de premier niveau de l'interface de l'agent : ffdc_date_time.N.log, exception_summary_date _heure.N.log	Traces et messages standard de l'interface de l'agent.
		console.log	Informations sur le démarrage, la session, la transaction et l'arrêt.
Informations système du serveur Cloud APM	/opt/ibm/ccm/systemInfoLogs	cpuinfo.log	Informations sur la configuration de l'unité centrale.
		df.log	Informations sur la configuration du disque.
		filelist.log	Liste des fichiers contenus dans les répertoires usr/servers/apmui, usr/servers/min et usr/servers/server1.
		hosts.log	Copie de etc/hosts.
		meminfo.log	Informations sur la configuration de la mémoire.
		opt-ibm-files.log	Liste des fichiers contenus dans le répertoire d'installation du produit.
		ps.log	Liste de tâches au moment de la collecte.
		rpm.log	Progiciels installés au moment de la collecte.
		sfdisk.log	Informations sur les volumes montés.
		ss.log	Sockets du réseau ouverts au moment de la collecte.
		timestamp.log	Date et heure de la collecte.
		ulimit.log	Valeur de ulimit au moment de la collecte.
		version.log	Informations sur la version de Linux.

Tableau 227. Fichiers journaux collectés par le script collectLogs.sh (suite).

Composant	Répertoire du journal	Nom du fichier journal	Description
Fournisseur de services OSLC	/opt/ibm/ccm/oslc_pm/logs	candle_installation.log	Les informations sur l'environnement d'installation collectées à chaque redémarrage sont incluses.
		UpdateAutoRun.log	Configure un environnement d'automatisation.
		hostname_as.inv	Index des fichiers journaux.
		hostname_as_NNNNNN.log	Fichier de trace du service OSLC Performance Monitoring.
Registre des composants de service	/opt/ibm/ccm/SCR/XMLToolKit/log	msgGTM_CI.log.N	
		msgGTM_XT.log.N	
		msgGTM_XT.log.N.lck	
		traceGTM_CI.log.N	
		traceGTM_XT.log.N	
		traceGTM_XT.log.N.lck	
	/opt/ibm/ccm/SCR/XMLToolkit/bin	xmltoolkitsvc.properties	Informations de configuration du kit d'outils XML.
	/opt/ibm/ccm/SCR/XMLToolkit/log/install/maintenance		Scripts de maintenance de base de données et informations SQL
MongoDB	/opt/ibm/mongodb/logs	mongodb.log	Journal principal MongoDB. MongoDB stocke les données d'événement de seuil et les données de suivi des transactions.
Courtier de messages Kafka	/opt/ibm/kafka/logs	controller.log	Journal du sous-système «controller» dans Kafka.
		kafka-request.log	Journal du sous-système «request» dans Kafka.
		server.log	Journal principal Kafka.
		state-change.log	Journal du sous-système «state-change» dans Kafka.
		kafka-server.err	Flux d'erreurs standard du processus Kafka.
		zookeeper-server.err	Flux d'erreurs standard du processus Zookeeper.
Base de données Derby du serveur Cloud APM	/opt/ibm/gaian	gaiandb.log	Informations sur le démarrage et les performances du noeud.
		derby.log	Informations sur le démarrage de la base de données Derby.
		*.properties	Informations sur la configuration de base de données.
Base de données Db2 utilisée par le serveur Cloud APM	/opt/ibm/db2/tbsmdb/logs		Fichiers journaux contenant les opérations Db2 qui ont été exécutées pendant l'installation du produit.

Tableau 227. Fichiers journaux collectés par le script collectLogs.sh (suite).

Composant	Répertoire du journal	Nom du fichier journal	Description
Couche de données du serveur Cloud APM	/opt/ibm/dtl/datalayer/logs		Fichiers journaux contenant les statistiques de performance Db2 pour la base de données DATAMART.
Installation de l'infrastructure Performance Management	/opt/ibm/ccm/logs	smai_oslc_pm-rpm _inst_trace.log IA_SCR_Install6.1.2-00.log deploymentResults.log apm-server-install _20150217_110258.log smai-apmui-configuration _trace.log smai-oslc-prestart.log configureMIN.log itmcdp.log db2setup_wse.log	Fichiers journaux d'installation.
Agent ksy	/opt/ibm/sy/logs		Fichiers journaux de l'agent ksy
serveur Db2	/home/db2apm/sqllib/db2dump		Fichiers journaux du serveur Db2
Installation de l'agent (Windows uniquement)	install_dir\logs	APMADV_Agents_install.log, IAPM_Agents_install.log, APD_Agents_install.log, APM_Agents_install.log	Fichiers journaux d'installation de l'agent.
Fournisseur OpenID Connect	/opt/ibm/wlp/usr/servers/oidc/logs	messages.log	Messages standard du fournisseur OpenID Connect.
Agents de serveur	/opt/ibm/serveragents/logs	Le répertoire contient plusieurs fichiers journaux. Pour trouver ceux qui concernent un agent spécifique, utilisez l'une des chaînes suivantes dans votre recherche : • S'il s'agit de l'Monitoring Agent for Bluemix Integration (biagent), recherchez *bi*. • S'il s'agit de l'agent de surveillance d'événements synthétiques (soagent), recherchez *so*. • S'il s'agit de l'agent de surveillance d'événement de transaction (txagent), recherchez *tx*.	Fichiers journaux des agents serveur.
Service de requête de diagnostic	/opt/ibm/wlp/usr/servers/dqe/logs	message.log, trace.log	Fichiers journaux du service de requête de diagnostic (dqe).
Système de back end de la console Performance Management (server1)			
Serveur Server1 principal	/opt/ibm/wlp/usr/servers/server1	server.xml, jvm.options, bootstrap.properties	Informations de configuration et machine virtuelle Java du serveur Server1.

Tableau 227. Fichiers journaux collectés par le script collectLogs.sh (suite).

Composant	Répertoire du journal	Nom du fichier journal	Description
Journaux de Server1	/opt/ibm/wlp/usr/servers/server1/logs	messages.log	Messages standard de Server1.
		trace.log	Journaux de trace de Server1.
		kd8collect*date*_*heure*.tar.gz	Archive contenant les informations de débogage du fournisseur de données.
		console.log	Sortie standard de Server1 contenant les informations sur le démarrage, la session, la transaction et l'arrêt.
		w7_audit.log	Journal d'audit du contrôle d'accès basé sur les rôles des modifications apportées aux artefacts liés à RBAC, telles que la création de droits et de rôles, l'affectation de droits à des rôles et l'affectation d'utilisateurs et de groupes d'utilisateurs à des rôles.
		scrderby.log	Informations sur le démarrage de la base de données Derby du référentiel des composants de service.
		scrserver.log	Journaux de processus du serveur du référentiel des composants de service.
		scrserver-errors.log	Messages d'erreur liés aux processus du serveur du référentiel des composants de service.
Outil de diagnostic de premier niveau de Server1	/opt/ibm/wlp/usr/servers/server1/logs/ffdc	ffdc_date_heure.N.log	Journaux de capture de données à la première défaillance.
		exception_summary_date_heure.N.log	Récapitulatifs des exceptions de traitement de l'outil de diagnostic de premier niveau.
Console Performance Management (interface utilisateur d'APM)			
Serveur principal de l'interface utilisateur APM	/opt/ibm/wlp/usr/servers/apmui	server.xml, jvm.options, bootstrap.properties	Informations de configuration et machine virtuelle Java du serveur console Cloud APM (interface utilisateur d'APM).

Tableau 227. Fichiers journaux collectés par le script collectLogs.sh (suite).

Composant	Répertoire du journal	Nom du fichier journal	Description
Journaux du serveur de l'interface utilisateur APM	`/opt/ibm/wlp/usr/servers/apmui/logs`	`messages.log`	Messages d'erreur standard du serveur de l'interface utilisateur APM.
		`trace.log`	Journal de trace du serveur de l'interface utilisateur APM.
		`console.log`	Sortie standard du serveur de l'interface utilisateur APM contenant les informations sur le démarrage, la session, la transaction et l'arrêt.
		`APM_UI.log`	Journal des processus de l'interface utilisateur d'APM.
		`derby.log`	Journal Derby de l'interface utilisateur d'APM.
		`itp.log`	Journal du portail informatique contenant les informations sur le client et le serveur.
Outil de diagnostic de premier niveau de l'interface utilisateur APM	`/opt/ibm/wlp/usr/servers/apmui/logs/ffdc`	`ffdc_date_heure.N.log`	Journaux de capture de données à la première défaillance.
		`exception_summary_date_heure.N.log`	Récapitulatifs des exceptions de traitement de l'outil de diagnostic de premier niveau.

Collecte des journaux d'agent de surveillance pour le support IBM

Utilisez l'outil de collecte d'identification de problème, *pdcollect*, pour rassembler les journaux requis et d'autres informations d'identification de problème demandées par le support IBM pour les agents de surveillance.

L'outil de collecte PD est installé avec chaque agent de surveillance.

Avant de commencer

Des droits d'administrateur ou root sont requis pour que l'outil de collecte PD puisse rassembler les informations système des agents de surveillance. Vous pouvez consulter les journaux des agents individuellement dans les dossiers suivants :

- Windows [64 bits] *rép_install*\TMAITM6_x64\logs
- Windows [32 bits] *rép_install*\TMAITM6\logs
- Linux AIX *rép_install*/logs

Restriction : Il n'est possible d'exécuter qu'une seule instance du script `pdcollect`.

Pourquoi et quand exécuter cette tâche

L'emplacement par défaut de *rép_install* est :

- Windows `C:\IBM\APM`
- Linux `/opt/ibm/apm/agent`
- AIX `/opt/ibm/apm/agent`

Pour exécuter l'outil de collecte PD, procédez comme suit :

Procédure

1. Sur la ligne de commande, accédez au répertoire de l'agent :
   - Linux AIX *rép_install*/bin
   - Windows *rép_install*\BIN
2. Exécutez la commande suivante :
   - Linux AIX **./pdcollect**
   - Windows **pdcollect**

   Un fichier dont le nom comporte un horodatage est généré dans le répertoire tmp, comme /tmp/pdcollect-nc049021.tar.Z.
3. Envoyez les fichiers de sortie à votre représentant du support IBM.

Fonctions d'accessibilité

Les fonctions d'accessibilité aident les utilisateurs souffrant d'un handicap (mobilité réduite ou vision limitée) à se servir des contenus des technologies de l'information.

Fonctions d'accessibilité

L'interface basée sur le Web d' IBM Cloud Application Performance Management est la console Cloud APM. Cette console comprend les principales fonctions d'accessibilité suivantes :

- Elle permet aux utilisateurs d'utiliser les technologies d'assistance, tels que le logiciel de lecture d'écran et le synthétiseur de parole numérique, pour entendre ce qui est affiché à l'écran. Consultez la documentation de la technologie d'assistance pour obtenir des détails sur son utilisation avec ce produit.
- Elle permet aux utilisateurs d'utiliser des fonctions spécifiques ou équivalentes en utilisant uniquement le clavier.
- Elle communique toutes les informations indépendamment de la couleur.[1]

La console Cloud APM utilise la dernière norme W3C, WAI-ARIA 1.0 (http://www.w3.org/TR/wai-aria/), pour assurer la conformité à US Section 508 (http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) et aux Règles pour l'accessibilité des contenus Web (WCAG) 2.0 . Pour tirer parti des fonctions d'accessibilité, utilisez la dernière version de votre lecteur d'écran de pair avec le navigateur Web le plus récent pris en charge par ce produit.

La documentation en ligne de la console console Cloud APM prend en charge les fonctions d'accessibilité dans l'IBM Knowledge Center. Les fonctions d'accessibilité de l'IBM Knowledge Center sont décrites à l'adresse : IBM Knowledge Center release notes .

Navigation au clavier

Ce produit utilise les touches de navigation standard.

Informations sur l'interface

L'interface utilisateur Web de la console Cloud APM n'utilise pas de feuilles de style en cascade pour un rendu correct du contenu et fournit une expérience utilisateur satisfaisante. C'est cependant le cas de la documentation du produit. L'IBM Knowledge Center fournit un moyen équivalent pour les utilisateurs malvoyants afin d'utiliser leurs paramètres d'affichage personnalisé, y compris le mode de contraste élevé. Il est possible de contrôler la taille de police dans les paramètres du périphérique ou du navigateur.

L'interface utilisateur Web de la console Cloud APM inclut des repères de navigation WAI-ARIA dont vous pouvez vous servir pour naviguer rapidement jusqu'aux zones fonctionnelles de l'application.

L'interface utilisateur de la console Cloud APM ne dispose pas de contenu qui clignote 2 à 55 fois par seconde.

1. Les exceptions incluent des pages **Configuration d'agent** de la console Performance Management.

© Copyright IBM Corp. 2015, 2018

Informations sur l'accessibilité associées

En plus de l'aide IBM standard et des sites Web de support, IBM a mis en place un support téléphonique par téléscripteur destiné aux utilisateurs sourds ou malentendants pour leur permettre d'accéder aux services de ventes et d'assistance :

TTY service 800-IBM-3383 (800-426-3383) (en Amérique du Nord)

IBM et l'accessibilité

Pour plus d'informations sur l'engagement d'IBM en matière d'accessibilité, consultez le site IBM Accessibility (www.ibm.com/able).

Remarques

Ces informations ont été développées pour des produits et services disponibles aux Etats-Unis. Pour vous procurer ces documents en d'autres langues, veuillez en faire la demande à IBM. Toutefois, vous devrez peut-être prouver que vous êtes propriétaire d'une copie de ce produit ou de cette version du produit dans cette langue pour prétendre à ces documents.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Une référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

© Copyright IBM Corp. 2015, 2018

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'IBM Customer Agreement, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance décrites dans le présent document ont été calculées en conditions de fonctionnement et d'environnement spécifiques. Les résultats peuvent donc varier.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme des objectifs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes ou de sociétés serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Ces exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM n'est en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright,
libellée comme suit :
© (nom de votre société) (année).

Des segments de code sont dérivés des Programmes exemples d'IBM Corp.
© Copyright IBM Corp. 2014, 2015.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines dans de nombreux pays. Les autres noms de produit et de service peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.



Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions s'ajoutent aux conditions d'utilisation du site Web d'IBM.

Usage personnel

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité sur Internet

Les logiciels IBM, y compris les Logiciels sous forme de services, («Offres Logiciels») peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Dans la plupart des cas, aucune information identifiant la personne n'est collectée par les Offres logicielles. Certaines de nos offres logicielles peuvent vous permettre de collecter des informations identifiant la personne. Si cette offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont énoncées dans les paragraphes ci-dessous.

En fonction des configurations déployées, cette offre logicielle peut utiliser des cookies de session qui collectent le nom d'utilisateur de chaque utilisateur à des fins de gestion des sessions, d'authentification et de configuration de la connexion unique. Ces cookies peuvent être désactivés, mais, en les désactivant, cela va aussi très probablement supprimer les fonctions qu'ils rendent possibles.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation des différentes technologies, y compris les cookies, à ces fins, voir IBM's Privacy Policy à l'adresse http://www.ibm.com/privacy et IBM's Online Privacy Statement à l'adresse http://www.ibm.com/privacy/details, ainsi que les sections «Cookies, Web Beacons and Other Technologies» et «IBM Software Products and Software-as-a-Service Privacy Statement» à l'adresse http://www.ibm.com/software/info/product-privacy.



Imprimé en France

SC43-4203-03

