IBM QRadar Network Packet Capture
Version 7.3.1

Guide d'administration

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 41.

Certaines illustrations de ce manuel ne sont pas disponibles en français à la date d'édition.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.1 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

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.

© Copyright IBM Corporation 2016, 2018.

Table des matières

© Copyright IBM Corp. 2016, 2018

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. 2016, 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.

Présentation de l'administration du produit QRadar Network Packet Capture

Les administrateurs utilisent IBM® QRadar Network Packet Capture pour gérer le tableau de bord.

Utilisateurs concernés

Ce guide est destiné à tous les utilisateurs QRadar Network Packet Capture chargés de l'étude et de la gestion de la sécurité réseau. Il suppose que vous avez accès à QRadar Network Packet Capture et que vous maîtrisez votre réseau d'entreprise et les technologies réseau.

Documentation technique

Pour trouver la documentation du produit IBM Security QRadar dans la bibliothèque des produits QRadar, voir la note technique Accessing IBM Security Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir la note technique Support and Download (en anglais) (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Instructions relatives aux bonnes pratiques de sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut être utilisé uniquement de façon réglementaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

© Copyright IBM Corp. 2016, 2018

1 Nouveautés pour les administrateurs dans QRadar Network Packet Capture version 7.3.1

IBM QRadar Network Packet Capture version 7.3.1 offre une possibilité d'empilage et une prise en charge SSH.

Stockage étendu pour l'empilage de données de capture de packet

L'empilage QRadar Network Packet Capture est utilisé pour connecter plusieurs dispositifs QRadar Network Packet Capture de manière à étendre le stockage disponible pour les données de capture. Par exemple, vous avez maintenant la possibilité d'empiler jusqu'à 16 dispositifs de stockage QRadar Network Packet Capture pour augmenter le délai de conservation de leurs données.

 En savoir plus sur la configuration de l'empilage QRadar Network Packet Capture...

Pour plus d'informations, voir le document *IBM QRadar Network Packet Capture - Guide d'utilisation*.

Prise en charge SSH de QRadar Network Packet Capture

Configurez le widget **SSH** pour activer l'accès à la ligne de commande SSH pour des utilisateurs QRadar Network Packet Capture spécifiques. Utilisez l'accès à la ligne de commande SSH pour vous aider dans vos opérations d'identification et résolution des problèmes et de débogage.

 En savoir plus sur l'identification et résolution des problèmes liés à QRadar Network Packet Capture...

Pour plus d'informations, voir le document *IBM QRadar Network Packet Capture - Guide d'utilisation*.

© Copyright IBM Corp. 2016, 2018

2 Administration de QRadar Network Packet Capture

Vous devez vous assurer d'être connecté en tant qu'administrateur lorsque vous effectuez des tâches de capture de paquet.

QRadar Network Packet Capture - Configuration des comptes utilisateur et de l'authentification

L'authentification utilisateur sur le dispositif IBM QRadar Network Packet Capture est un processus à deux étapes. Lorsqu'un utilisateur tente de se connecter, l'authentification est effectuée localement. En cas d'échec de l'authentification, l'utilisateur est authentifié via un serveur Active Directory or Lightweight Directory Access Protocol (LDAP) configuré. Si ces deux types d'authentification échouent, l'accès est refusé à l'utilisateur.

Remarque : Si le dispositif QRadar Network Packet Capture est membre d'un groupe QRadar Network Packet Capture, les configurations de compte utilisateur et d'authentification sont automatiquement synchronisées dans l'ensemble du groupe.

Création d'un utilisateur local

Si le nombre d'utilisateurs est peu élevé et que vous n'avez pas besoin de fournisseur d'authentification (serveur Active Directory ou LDAP, par exemple), créez un compte de connexion local pour chaque utilisateur ayant besoin d'accéder au dispositif IBM QRadar Network Packet Capture.

Avant de commencer

Connectez-vous au dispositif QRadar Network Packet Capture en tant qu'administrateur.

L'unité QRadar Network Packet Capture prend également en charge l'authentification utilisateur intégrale en configurant les services Microsoft Active Directory ou LDAP. Voir «Configuration d'un serveur Active Directory ou LDAP pour l'authentification d'utilisateur», à la page 4.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Accédez au widget ACCOUNTS et entrez des valeurs dans les zones **user** et **password** pour le nouvel utilisateur.
3. Sélectionnez un niveau utilisateur :
   - Pour les administrateurs ayant besoin du niveau d'accès le plus élevé et pouvant modifier les configurations, sélectionnez **Admin**.
   - Pour les utilisateurs ayant besoin d'utiliser le dispositif QRadar Network Packet Capture pour les utilisations opérationnelles (recherches et requêtes, par exemple), sélectionnez Opérateur.
   - Pour les utilisateurs ayant besoin de contrôler les résultats du dispositif QRadar Network Packet Capture, sélectionnez Contrôleur.

   Utilisez les informations suivantes pour déterminer le niveau utilisateur requis :

Activité	Niveau Moniteur	Niveau Opérateur	Niveau Admin
Obtention d'informations de statistiques à partir de l'unité	X	X	X
Obtention d'informations sur la configuration du groupe en cours	X	X	X

© Copyright IBM Corp. 2016, 2018

Activité	Niveau Moniteur	Niveau Opérateur	Niveau Admin
Lancement d'une recherche et d'une requête de données à partir de l'unité		X	X
Annulation d'une recherche en cours		X	X
Modification de la configuration pour l'unité (ajout ou retrait d'un compte utilisateur, par exemple)			X
Réinitialisation/suppression des informations de statistiques concernant l'unité			X
Obtention d'informations de support, incluant les journaux et l'archive de support, à partir de l'unité			X
Démarrage et arrêt de la capture des données			X
Modification de la configuration de groupe			X

4. Cliquez sur **Add account**.

Changement du mot de passe de l'utilisateur local

Pour des raisons de sécurité, vous pouvez changer le mot de passe des utilisateurs en utilisant le widget ACCOUNTS.

Pourquoi et quand exécuter cette tâche

L'utilisateur local est automatiquement déconnecté lorsque vous changez le mot de passe. L'utilisateur doit se connecter à nouveau en utilisant le nouveau mot de passe. Lorsqu'un administrateur change son propre mot de passe, il doit également se connecter à nouveau.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Accédez au widget ACCOUNTS et entrez le nom d'utilisateur approprié dans la zone **user**.
3. Entrez le nouveau mot de passe dans la zone **password** puis cliquez sur **Update Account**. Une confirmation s'affiche et le nouveau mot de passe prend immédiatement effet.

Configuration d'un serveur Active Directory ou LDAP pour l'authentification d'utilisateur

IBM QRadar Network Packet Capture est intégré à votre infrastructure de sécurité via votre fournisseur d'authentification existant. Utilisez le widget AUTHENTICATION AND AUTHORIZATION pour configurer Active Directory et LDAP. QRadar Network Packet Capture prend en charge l'authentification d'utilisateur complète, comme cela est spécifié par les services Microsoft Active Directory ou un service LDAP. Microsoft Active Directory et les serveurs LDAP en tant que source d'authentification sont désactivés par défaut.

Avant de commencer

Connectez-vous à l'unité QRadar Network Packet Capture en tant qu'administrateur.

Procédure

1. Cliquez sur l'onglet **ADMIN** et accédez au widget AUTHENTICATION AND AUTHORIZATION.
2. Sélectionnez le type de serveur approprié puis cliquez sur **Apply**. Les paramètres que vous pouvez configurer dépendent du type de serveur d'authentification.

Remarque : Si le serveur d'authentification et d'autorisation principal est inaccessible lorsqu'un serveur demande l'authentification, une recherche de nom DNS est effectuée dans les enregistrements de service (SRV). Les adresses IP SRV résolues répertoriées sont utilisées comme serveurs d'authentification secondaires.

Important : Si Active Directory est activé, le nom d'utilisateur doit être un nom de domaine complet (par exemple, `\\[domaine]\[nom utilisateur]` ou `[nom utilisateur]@[domaine]`).

Utilisez le tableau suivant pour choisir et configurer le type de serveur.

Paramètre	Type de serveur	Description	Valeur par défaut
Protocole pour la communication avec le serveur Active Directory ou LDAP	Tous	Protocole et méthode de chiffrement. Valeurs possibles : • LDAP • LDAP + TLS • LDAP + SSL	LDAP
Nom d'hôte ou adresse IP du serveur Active Directory ou LDAP	Tous		N/A
Numéro de port pour la connexion au serveur Active Directory ou LDAP	Tous		389
Délai, en secondes, pour la connexion au serveur Active Directory ou LDAP	Tous		25 secondes
Nom de domaine de base	Tous	Nom distinctif de l'emplacement où la requête doit être démarrée.	N/A
Groupe de niveau administrateur	Tous	Nom du groupe utilisé pour l'identification des privilèges de niveau administrateur	N/A
Groupe de niveau opérateur	Tous	Nom du groupe permettant d'identifier les privilèges de niveau opérateur	N/A
Groupe de niveau moniteur	Tous	Nom du groupe utilisé pour l'identification des privilèges de niveau moniteur	N/A
Filtre	LDAP	Condition devant être remplie par les entrées	N/A
Portée du filtre	LDAP	Valeurs possibles : • Base • Un niveau • Sous-arborescence	Sous-arborescence
Nom d'attribut utilisé pour l'affectation de groupes à des utilisateurs	LDAP	Nom de l'attribut des objets renvoyés contenant les noms de groupe	

Paramètre	Type de serveur	Description	Valeur par défaut

Base utilisateur LDAP utilisée lors de la liaison à un serveur LDAP	LDAP	Spécifiez les informations d'authentification pour autoriser des utilisateurs à se connecter avec un nom d'utilisateur abrégé.
		
		Vous pouvez, par exemple, spécifier :
		
		`cn={},dc=company,dc=com`
		
		où {} correspond au nom d'utilisateur (par exemple, `admin`) et `company.com` à votre domaine.
		
		Autre exemple :
		
		`uid={},ou=people,`
		
		`dc=company,dc=com`
		
		Lorsque la zone `USERBASE` est définie, un utilisateur peut se connecter en utilisant son nom d'utilisateur abrégé, (par exemple, `admin`) sans avoir à spécifier un nom de domaine complet.	

Vérification de la cohérence des données au démarrage

L'intégrité et la cohérence des données stockées sont vérifiées au démarrage du dispositif IBM QRadar Network Packet Capture.

Un message s'affiche après la connexion à QRadar Network Packet Capture indiquant que le service est en cours d'initialisation. Une barre d'état dans la partie supérieure de la fenêtre présente la progression de l'initialisation.

La durée de la vérification de la cohérence dépend de la quantité de données stockées sur le dispositif QRadar Network Packet Capture.

Configuration de la date et de l'heure (NTP)

Pour vous assurer que les données capturées sont correctement horodatées, vous devez configurer la date et l'heure utilisées par QRadar Network Packet Capture. Vous pouvez configurer une date et une heure locales pour QRadar Network Packet Capture, ou permettre au protocole NTP (Network Time Protocol) ou au protocole PTP (Precision Time Protocol) de synchroniser la date et l'heure à partir d'une source externe.

Avant de commencer

Vérifiez qu'aucun câble PTP n'est relié à l'unité QRadar Network Packet Capture.

Si vous modifiez le paramétrage de l'heure système, vous devez désactiver la capture de données avent d'installer des mises à jour.

Si la différence d'heure attendue est importante (plus d'une minute), redémarrez l'unité QRadar Network Packet Capture après la mise à jour pour que tous les sous-systèmes soient synchronisés.

En cas de différence négative, effacez toutes les données capturées avant la mise à jour pour éviter des problèmes d'horodatage.

Procédure

1. Cliquez sur l'onglet **ADMIN** puis accédez au widget NTP SETUP.

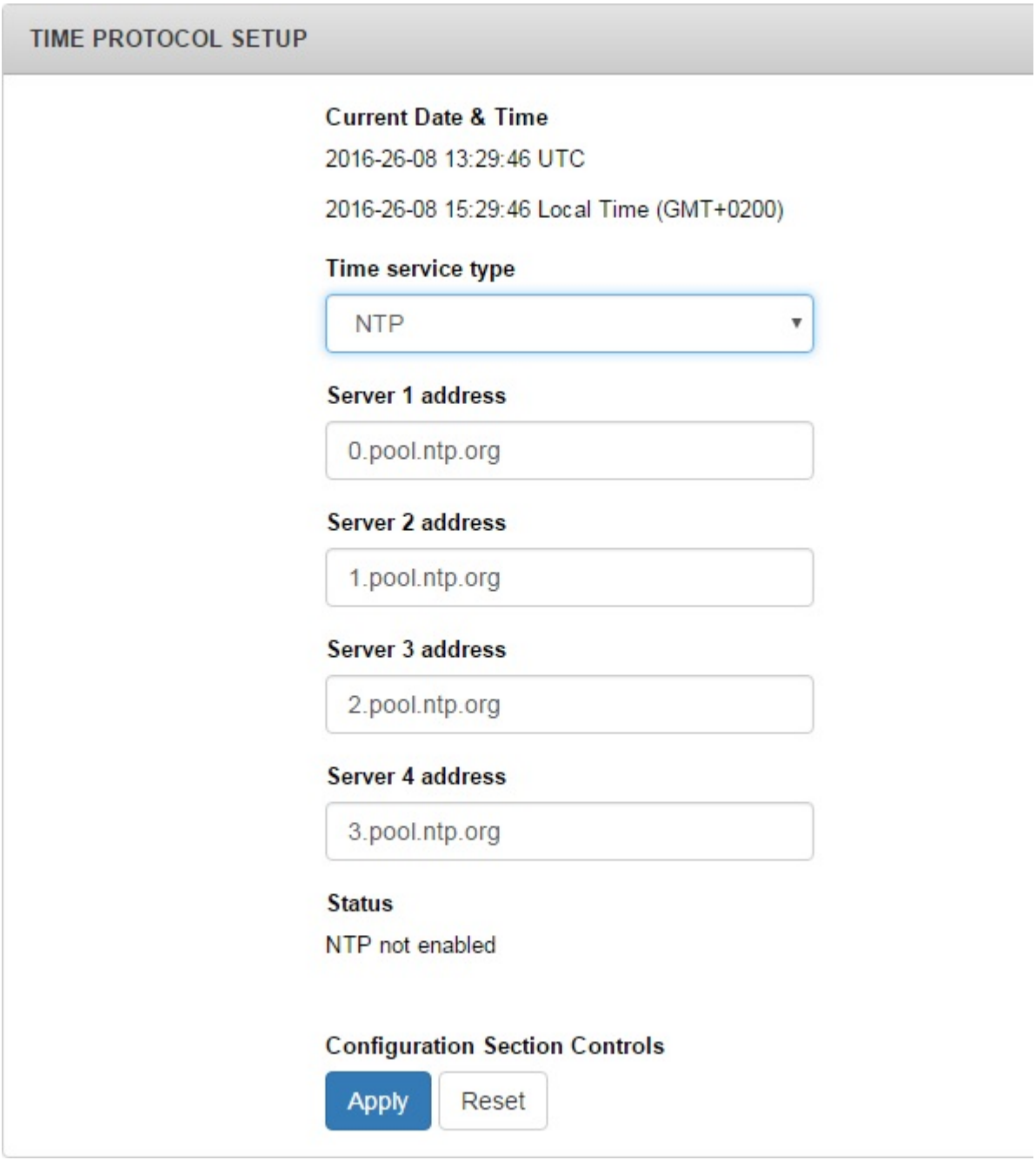


Figure 1. Widget Time Protocol Setup

2. Pour configurer une date et une heure locales, entrez la date et l'heure au format décrit dans la zone appropriée.

3. Sélectionnez un type de service de gestion de l'heure en fonction de vos besoins :

Tableau 1. Configuration du type de service de gestion de l'heure

Type de service de gestion de l'heure	Description
NTP	Synchronise l'heure et la date avec un serveur externe.
RDate	Synchronise la date et l'heure en cours à partir d'un serveur réseau.
Manuel	Entrez la date et l'heure au format ISO8601 ou `jj/mm/aaaa h:m:s`.

4. Sélectionnez les adresses de serveur pertinentes pour les sources de date et d'heure.
5. Cliquez sur **Apply** pour terminer le processus.

Résultats

L'accélérateur se trouvant dans QRadar Network Packet Capture synchronise automatiquement l'heure en fonction de l'heure du système d'exploitation.

Configuration des noms d'emplacement et de contact

Pour identifier plus facilement le dispositif QRadar Network Packet Capture, assurez-vous de lui avoir attribué un nom reconnaissable.

Procédure

1. Cliquez sur l'onglet **ADMIN**.
2. Faites défiler jusqu'au widget GENERAL SETUP, comme présenté ci-dessous.

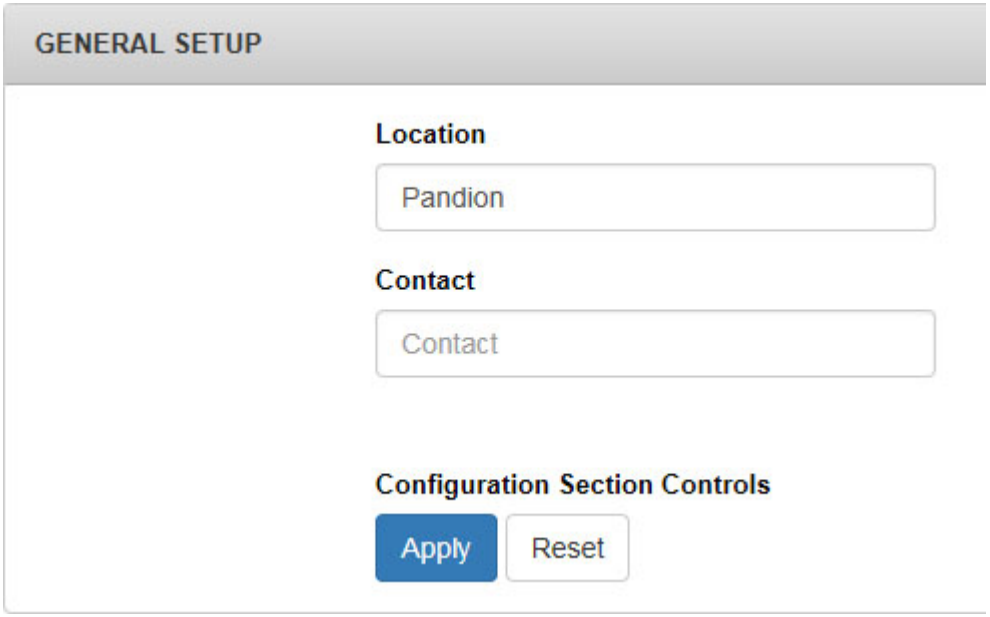


Figure 2. Widget de configuration générale

3. Entrez un nom d'emplacement et éventuellement le nom d'une personne à contacter.
4. Cliquez sur **Apply**.

Démarrage ou arrêt d'une opération de capture de paquet

Vous pouvez contrôler le nombre d'enregistrements capturés par votre dispositif.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Accédez au widget CONTROL.
3. Sélectionnez **Turn On** ou **Turn Off** pour l'option **Traffic Capture**.

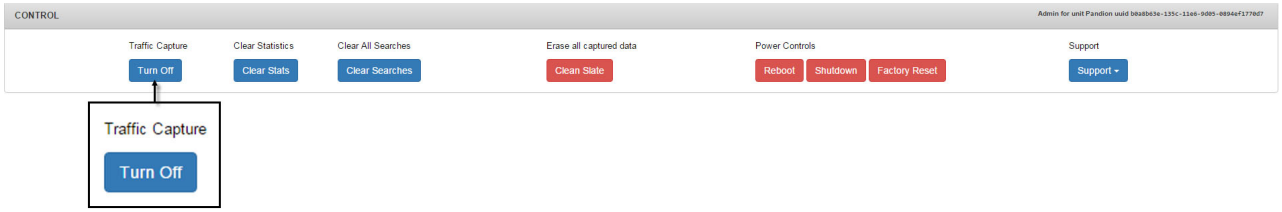


Figure 3. Capture de trafic

Par défaut, la capture de paquet est activée. Si QRadar Network Packet Capture ne capture pas de paquets, la valeur **Turn On** est sélectionnée pour l'option **Traffic Capture**. Si QRadar Network Packet Capture capture des paquets, la valeur **Turn Off** est sélectionnée pour l'option **Traffic Capture**.

Configuration du journal système distant

Le widget REMOTE SYSLOG SETUP permet d'activer la journalisation système distante et de configurer les détails de protocole.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Accédez au widget REMOTE SYSLOG SETUP.
3. Sélectionnez la case à cocher **Remote Syslog Enabled** pour activer la journalisation système.

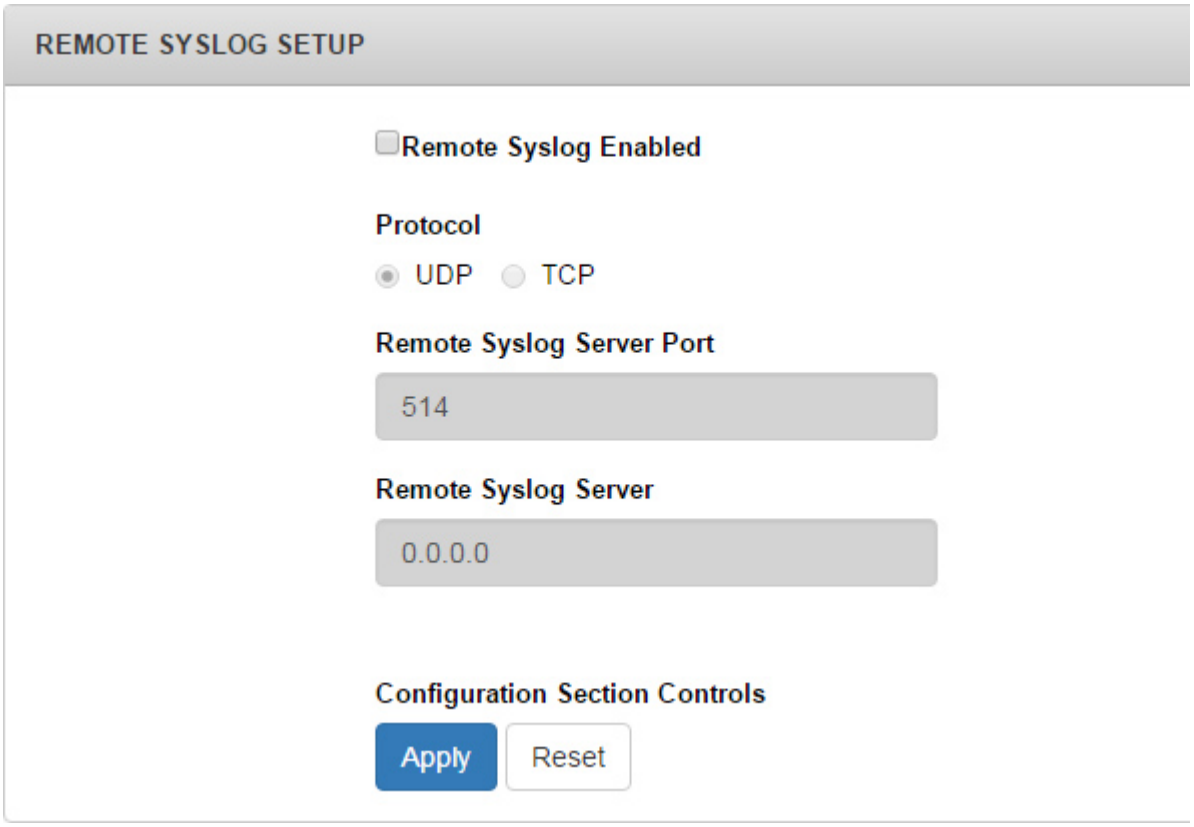


Figure 4. Configuration du journal système distant

4. Sélectionnez le protocole **UDP** ou **TCP**, en fonction de vos paramètres.
5. Indiquez un numéro de port dans la zone **Remote Syslog Server Port** et une adresse IP dans la zone **Remote Syslog Server**.
6. Cliquez sur **Apply**.

Affichage des journaux système

Utilisez SYSLOGS pour identifier et résoudre les problèmes liés à l'unité.

Par défaut, le widget SYSLOGS affiche les 500 dernières lignes du journal système du dispositif IBM QRadar Network Packet Capture.

Vous pouvez filtrer et définir le nombre de lignes affichées en utilisant les options **Syslog Level** et **Log Lines**.

Configuration de SNMP

Utilisez le widget GUI SNMP SETUP pour configurer SNMP pour le dispositif QRadar Network Packet Capture.

Vous pouvez inclure l'adresse IP cible à laquelle envoyer les alertes SNMP.

Pour plus d'informations sur les alertes SNMP, voir le document Dell OpenManage SNMP Reference Guide Version 7.2 ou recherchez *Dell OpenManage SNMP* avec votre moteur de recherche favori.

Configuration X509

Utilisez le widget X509 SETUP pour installer un nouveau certificat X509 utilisé par HTTPS pour authentifier le dispositif IBM QRadar Network Packet Capture.

Un certificat usine unique par unité est utilisé lorsqu'il n'existe aucun certificat installé par l'utilisateur. Le certificat est auto-signé.

Configuration de l'accélérateur

Le widget ACCELERATOR SETUP permet de configurer les paramètres du port d'accélérateur, le traitement des paquets ainsi que les pré-filtres.

Paramètres de port

Si un module SFP ou SFP+ est installé sur un port, il est activé par défaut. Vous pouvez désactiver manuellement le module dans le widget ACCELERATOR SETUP. Par défaut, chaque port détecte automatiquement la vitesse du module. Cependant, si vous utilisez des modules à double débit, vous pouvez définir manuellement la vitesse 1G ou 10G en utilisant les boutons d'option.

Le tableau suivant décrit la configuration de la fonction des différents ports.

Tableau 2. Configuration du paramétrage de la fonction des ports

Paramétrage de la fonction du port	**Description**
Capture	Paramétrage par défaut. Les paquets sont capturés.
Disabled	La capture des paquets est désactivée. Les paquets ne sont pas capturés.
Retransmit on ring	Les paquets sont retransmis à un autre port local. Sélectionnez le port vers lequel vous voulez les réacheminer.
Retransmit ETS	Un horodatage encapsulé (ETS - Encapsulated Time Stamp) est ajouté à chaque paquet, et tous les paquets sont retransmis à un autre port local.

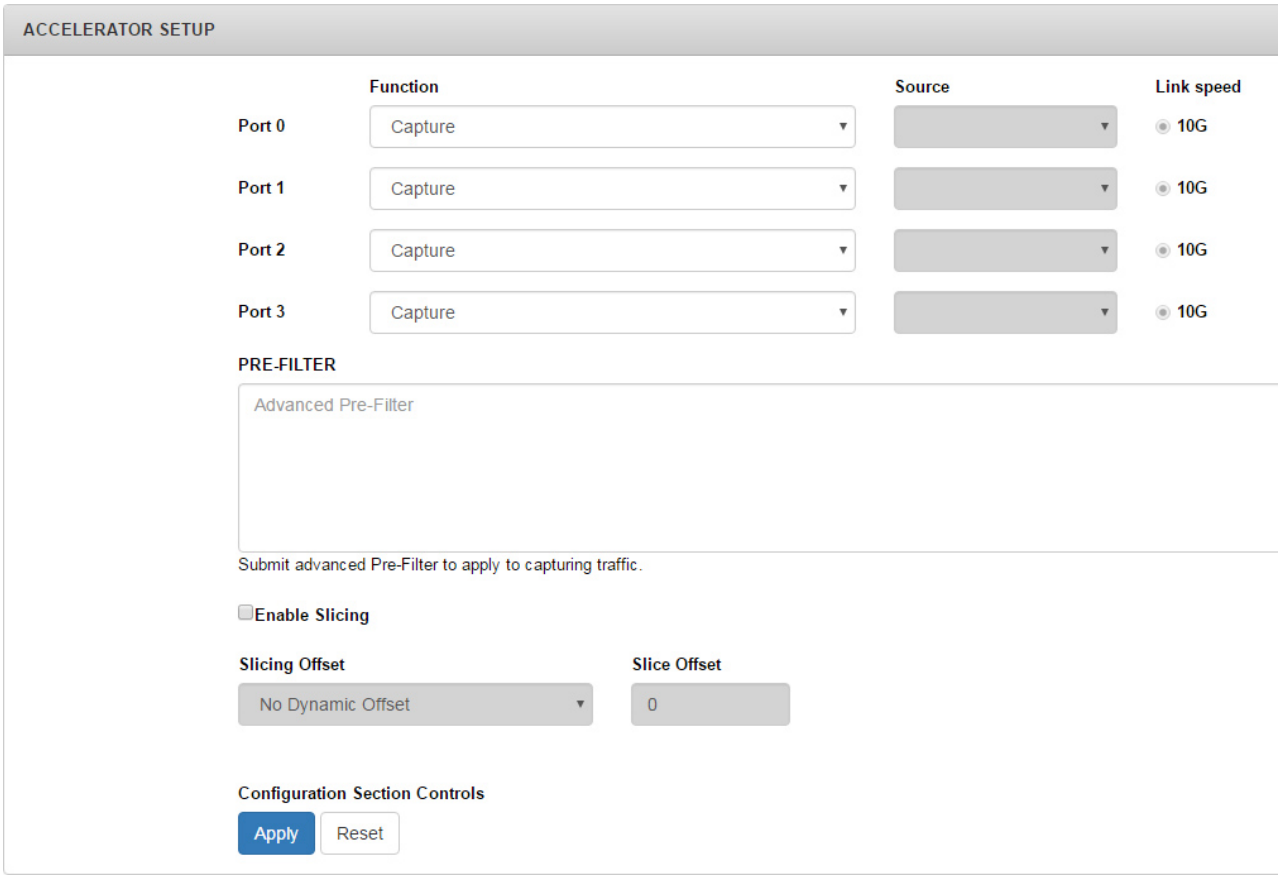


Figure 5. Configuration de l'accélérateur

Configuration des préfiltres

Le widget ACCELERATOR SETUP permet de filtrer les paquets capturés afin de réduire la taille des paquets capturés et stockés.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Accédez au widget ACCELERATOR SETUP.
3. Configurez les préfiltres:
   a. Entrez votre instruction dans la zone **PRE-FILTER**.
   b. Cliquez sur **Appliquer**.
4. Configurez le traitement des paquets :
   a. Entrez votre instruction dans la zone **PRE-FILTER**.
   b. Sélectionnez **Enable Slicing** et paramétrez le décalage pour activer le fractionnement. Le décalage de fractionnement présente un décalage dynamique ainsi qu'un décalage statique permettant le fractionnement de tous les paquets.
   c. Cliquez sur **Apply**.

Configuration de la retransmission locale

La retransmission locale du trafic permet d'envoyer les paquets reçus sur une interface réseau (un port physique) à une ou plusieurs interface réseau. Par exemple, vous pouvez retransmettre au port 2 tous les paquets reçus sur le port 1.

Insérez l'unité QRadar Network Packet Capture entre un tap réseau existant et un périphérique réseau. En activant la retransmission locale, vous pouvez recevoir l'ensemble du trafic dans l'unité QRadar Network Packet Capture et le réacheminer au périphérique réseau connecté.

La retransmission d'un paquet n'affecte pas sa capture.

L'unité QRadar Network Packet Capture retransmet le trafic aux ports sélectionnés.

Suppression des statistiques ou des recherches

Le widget CONTROL permet d'effacer toutes les recherches en cours et placées en file d'attente.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Accédez au widget CONTROL.
3. Sélectionnez **Clear Stats** dans la zone **Clear Statistics** si vous souhaitez effacer les données d'historique.
4. Sélectionnez **Clear Searches** dans la zone **Clear All Searches** si vous souhaitez effacer toutes vos recherches récentes.

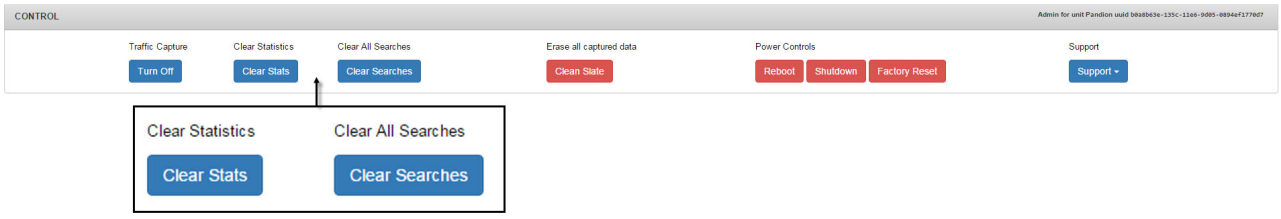


Figure 6. Suppression des statistiques ou des recherches.

Redémarrage du dispositif et restauration des valeurs d'usine

Le widget **CONTROL** permet d'accéder aux paramètres d'alimentation IBM QRadar Network Packet Capture.

Procédure

1. Pour redémarrer ou arrêter le dispositif QRadar Network Packet Capture, procédez comme suit :
   a. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
   b. Accédez au widget CONTROL.
   c. Sélectionnez **Reboot** ou **Shut Down** pour l'option **Power Controls**.

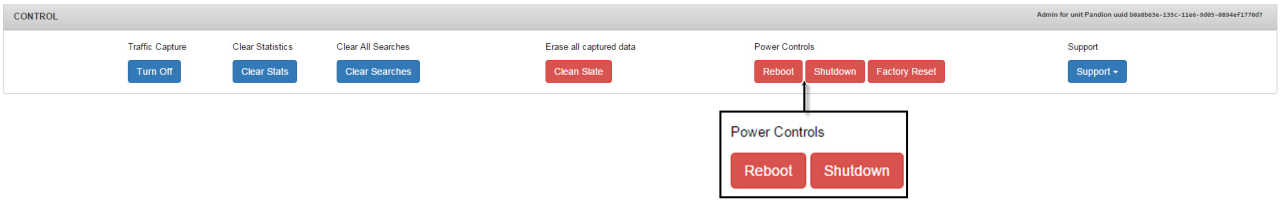


Figure 7. Contrôles de l'alimentation

2. Pour effacer des paquets réseau et restaurer les valeurs d'usine :
   a. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
   b. Accédez au widget CONTROL.
   c. Pour effacer des paquets réseau dans un tableau de disques RAID, sous **Erase all captured data**, sélectionnez **Clean Slate**.

      Remarque : Cette action supprime les données, mais ce n'est pas un effacement sécurisé. Elle n'effectue pas plusieurs passages et ne comporte pas d'algorithmes d'effacement sécurisé.
   d. Pour réinitialiser le dispositif QRadar Network Packet Capture, sous **Power controls**, sélectionnez **Factory Reset**.

      Remarque : L'option **Factory Reset** efface toutes les données capturées et restaure tous les paramètres, à l'exception de la configuration réseau.

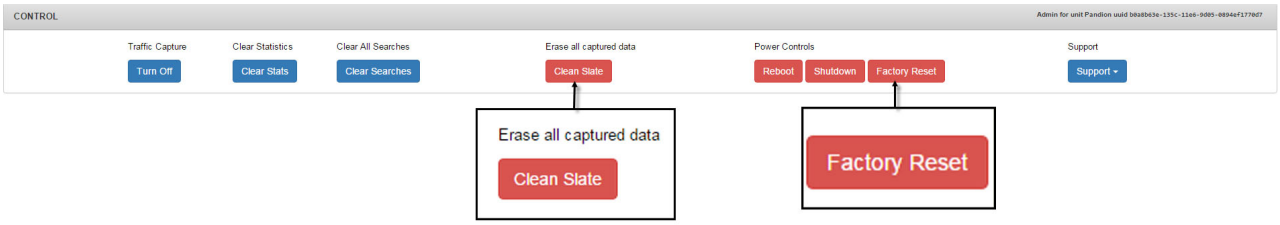


Figure 8. Contrôles de l'alimentation

Configuration de SSH

Vous pouvez activer l'accès à la ligne de commande SSH pour vous aider dans vos opérations d'identification et résolution des problèmes et de débogage. Utilisez le widget SUPPORT LOGIN (SSH) pour accorder l'accès à des utilisateurs spécifiques. Par défaut, la prise en charge SSH est toujours désactivée. Pour autoriser la prise en charge SSH, un certificat de clé fourni par le service clients est requis.

Procédure

1. Dans QRadar Network Packet Capture, cliquez sur l'onglet **ADMIN**.
2. Sélectionnez **Support** > **Enable Support Login (SSH)** dans le widget **CONTROL**

   Lorsque la prise en charge SSH est activée, toute personne détenant le certificat de clé et le mot de passe requis peut accéder au système pour la session active (ou jusqu'à ce que SSH soit désactivé en sélectionnant **Support** > **Enable Support Login (SSH)**). Lorsque l'hôte est réamorcé, SSH est automatiquement désactivé et l'utilisateur doit réactiver SSH.
3. Vous pouvez restreindre l'accès à SSH pour des adresses IP spécifiques à l'aide du widget SUPPORT LOGIN (SSH) ou en procédant comme suit :
   a. Cliquez sur l'onglet **ADMIN**.

b. Accédez au widget SUPPORT LOGIN (SSH).
c. Entrez des adresses IP, une par une, puis cliquez sur **Ajouter**.

Résultats

Le comportement de SSH se modifie comme suit :

- Seules les adresses spécifiées ont accès au système.
- La prise en charge SSH est activée en permanence pour ces adresses ; l'accès à SSH est donc activé par défaut après un redémarrage du dispositif.

3 QRadar Network Packet Capture et surveillance de la capture de paquet

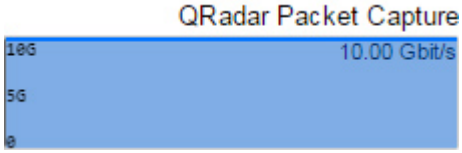
Les widgets de surveillance du tableau de bord présentent le statut général d'un ou de plusieurs dispositifs IBM QRadar Network Packet Capture d'un groupe.

Un groupe QRadar Network Packet Capture inclut des dispositifs, qui capturent des données provenant de différents taps réseau. Utilisez le regroupement pour former une entité logique plus facile à gérer et dans laquelle les recherches sont plus simples. Un groupe peut inclure jusqu'à huit dispositifs QRadar Network Packet Capture.

GROUP VIEW

Chaque dispositif QRadar Network Packet Capture se compose des composants de surveillance suivants :

Tableau 3. Composants de surveillance

Icône	Description
	Accélérateur
	Système
	Stockage
	Trafic

L'état du composant est indiqué par sa couleur (gris clair, jaune et rouge).

GROUP LIST VIEW

Le widget GROUP LIST VIEW permet de surveiller l'état de chaque dispositif QRadar Network Packet Capture du groupe.

UNIT VIEW

Le widget UNIT VIEW permet d'accéder à des informations détaillées supplémentaires sur le dispositif IBM QRadar Network Packet Capture sélectionné dans le widget GROUP VIEW.

Le widget UNIT VIEW présente des informations détaillées sur l'état du dispositif et de la conservation pour le dispositif QRadar Network Packet Capture.

Informations plus détaillées sur l'accélérateur, le système et le stockage.

© Copyright IBM Corp. 2016, 2018

CPU UTILIZATION

Le widget CPU UTILIZATION permet de surveiller individuellement l'utilisation de l'unité centrale pour chaque coeur multithread. Identifiez l'unité centrale en utilisant la vitesse et le modèle qui s'affichent.

TRAFFIC

Le widget TRAFFIC permet de surveiller l'historique du trafic de capture de paquet reçu par le dispositif QRadar Network Packet Capture.

Le graphique est mis à jour de manière périodique. La partie droite est présentée, affichant uniquement la dernière période des données d'historique.

PACKET DISTRIBUTION

Le widget PACKET DISTRIBUTION permet de surveiller la distribution entre les trames de diffusion, de multidiffusion et monodiffusion reçus par le dispositif IBM QRadar Network Packet Capture depuis la dernière réinitialisation des données statistiques.

PACKET SIZE DISTRIBUTION

Le widget PACKET SIZE DISTRIBUTION permet de surveiller la distribution des tailles de paquet pour les trames reçues par le dispositif QRadar Network Packet Capture depuis la dernière réinitialisation des données statistiques.

4 Requêtes et recherches QRadar Network Packet Capture

Pour rechercher des paquets spécifiques pendant une période définie et sur un port, utilisez l'onglet SEARCH. Lorsque vous définissez des zones d'adresse IP source, d'adresse IP cible, de port source, de port cible ou de port, une chaîne NTQL (QRadar Network Packet Capture Query Language) est générée. Vous pouvez modifier cette chaîne ou créer vous-même votre propre expression NTQL.

Par exemple, pour optimiser NTQL, remplacez `dst host` par `host` ou modifiez l'expression `and` en `or` entre les adresses IP source et de destination.

Limitation des résultats de la recherche

Pour limiter les résultats de la recherche et réduire la durée nécessaire à l'obtention des résultats, ajoutez une portée à la recherche en utilisant un des filtres suivants :

- Intervalle de temps
- Ports de réception (ports sélectionnés)

Si vous effectuez une recherche dans un groupe de dispositifs QRadar Network Packet Capture, soumettez les requêtes de recherche uniquement lorsque vous êtes connecté sur le dispositif local. Sinon, les performances d'extraction des résultats de recherche sont ralenties.

Les formats du résultat de recherche sont PCAP standard et PCAP-NG. Le format PCAP-NG contient des informations de numéro de port, même pour les recherches effectuées dans un groupe de dispositifs QRadar Network Packet Capture. Pour chaque serveur du groupe, vous pouvez également spécifier les ports reçus pour la recherche de trafic.

Des informations de séquence de contrôle de trame (FCS, Frame Check Sequence) sont également renvoyées dans ce résultat de recherche. Ces informations sont envoyées en supplément des données de paquet.

Avant de soumettre la recherche, vous pouvez la mettre en file d'attente lorsque le moteur de recherche est occupé. Vous pouvez également choisir si la sortie doit être téléchargée automatiquement dès la fin de l'opération et définir la priorité des différentes recherches.

Différences entre NTQL et BPF

Utilisez NTQL pour accélérer les recherches en fonction de l'index généré pendant la capture.

Le fonctionnement des filtres NTQL est différent de celui des filtres BPF (Berkeley Packet Filter). Les exemples suivants décrivent le fonctionnement des filtres NTQL :

- Lorsque vous recherchez une adresse IP, tous les paquets ayant cette adresse IP sont renvoyés, quel que soit le balisage VLAN, MPLS ou ISL ou l'encapsulation.
- Lorsque vous recherchez des ports TCP ou UDP spécifiques, les résultats renvoyés incluent des paquets IPv6 avec des en-têtes étendus.

Le post-filtrage BPF est effectué en utilisant la syntaxe BPF complète. Créez l'expression BPF et ces filtres de post-filtrage BPF uniquement pour les paquets utilisant le filtre NTQL indiqué.

Les filtres BPF fonctionnent différemment des filtres NTQL et peuvent supprimer des paquets détectés par le filtre NTQL.

Concepts associés:

© Copyright IBM Corp. 2016, 2018

«NTQL», à la page 23
5, «Dispositifs QRadar Network Packet Capture regroupés», à la page 27

Recherches placées en file d'attente

Les recherches placées en file d'attente sont utilisées lorsque vous souhaitez exécuter plusieurs recherches.

Seule une recherche en cours à la fois est autorisée mais vous pouvez exécuter plusieurs recherches, qui sont ensuite placées en file d'attente et exécutées en fonction de la priorité. Ces recherches sont disponibles dans le widget SEARCH QUEUE.

L'image suivante présente une requête de recherche se trouvant en file d'attente qui sera exécutée en fonction de la priorité.

Figure 9. Widget SEARCH QUEUE.

Avant de soumettre la recherche, sélectionnez l'option **Auto-download when ready to stream**. Le résultat de la recherche est automatiquement téléchargé à la fin de la recherche. Vous pouvez changer ce comportement en cliquant sur **Auto Download is On**.

ACTIVE SEARCH

Le widget ACTIVE SEARCH présente les recherches actives et en cours.

L'image suivante présente une requête de recherche active.

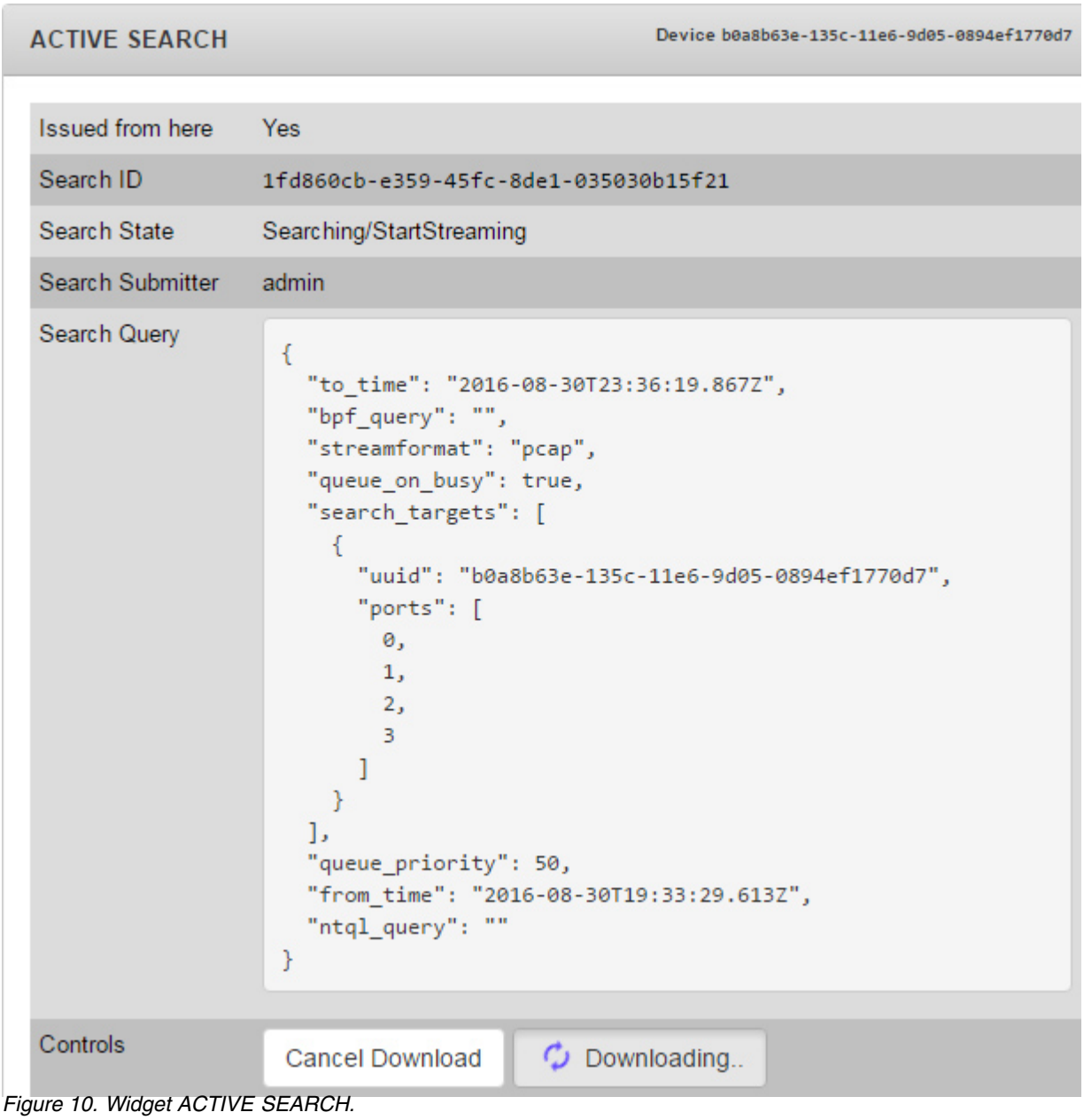


Figure 10. Widget ACTIVE SEARCH.

SEARCH HISTORY

Le widget SEARCH HISTORY inclut l'historique de recherche du dispositif IBM QRadar Network Packet Capture.

L'image suivante présente l'historique de recherche d'une requête de recherche terminée.

Figure 11. Widget SEARCH HISTORY

Modèle de recherche

En utilisant le widget SEARCH HISTORY, vous pouvez utiliser une recherche précédemment exécutée en tant que modèle pour une recherche ultérieure. Cliquez sur **Use as Search Template** et accédez au widget SEARCH afin d'apporter les modifications nécessaires au modèle.

Suppression de recherche

Vous pouvez arrêter une recherche mise en file d'attente en cliquant sur **Cancel Queued Entry** dans le widget SEARCH QUEUE. Vous pouvez arrêter une recherche active en cliquant sur **Cancel Search** dans le widget ACTIVE SEARCH.

NTQL

Utilisez QRadar Network Packet Capture Query Language (NTQL) pour extraire des données des paquets capturés. Par exemple, vous pouvez utiliser NTQL pour les types d'informations suivants :

- Adresses hôte IPv4, en tant que source, cible ou les deux
- Adresses hôte IPv6, en tant que source, cible ou les deux
- Numéros de port TCP ou UDP, en tant que source, cible ou les deux
- Protocole de couche 3 pris en charge par des trames Ethernet
- Protocole de couche 4 pris en charge par des packages IP
- Combinaison de ces éléments avec les opérateurs AND et OR logiques

Remarque : NTQL est sensible à la casse.

Correspondance globale

Une chaîne NTQL vide correspond à tous les paquets, ce qui est utile lorsque le nombre de correspondances est limité.

Recherche d'adresse hôte

Pour rechercher les paquets envoyés à un hôte spécifique, entrez la chaîne suivante :

```
src host
<adresse_IP>
```

Pour rechercher les paquets envoyés depuis un hôte, entrez la chaîne suivante :

```
dst
host <adresse_IP>
```

Recherche de numéro de port

Pour rechercher les paquets envoyés d'un port TCP ou UDP ou reçus sur ce dernier, entrez la chaîne suivante :

```
port <numéro>
```

Les paquets envoyés via des protocoles n'ayant pas de numéro de port sont ignorés par cette recherche.

Pour restreindre les résultats de la recherche aux paquets envoyés d'un port spécifique, entrez la chaîne suivante :

```
src
port <numéro>
```

Pour rechercher les paquets envoyés à un port spécifique, entrez la chaîne suivante :

```
dst
port <numéro>
```

Recherche de protocole de couche 3

Pour rechercher les paquets qui utilisent un protocole de couche 3 spécifique, entrez la chaîne suivante :

```
l3proto
<protocole>
```

où <*protocole*> correspond à un numéro de protocole ou à un nom. Les noms de protocole pris en charge sont les suivants :

- `ip`

- ip4
- ipv4
- arp
- ip6
- ipv6
- lldp
- ptp

Lorsque l'élément ip est spécifié en tant que protocole, le protocole IPv4 est utilisé.

Recherche de protocole de couche 4

Pour rechercher les paquets qui utilisent un protocole de couche 4 spécifique, entrez la chaîne suivante :

```
l4proto
<protocole>
```

où <*protocole*> correspond à un numéro de protocole ou à un nom. La liste suivante présente les noms pris en charge :

3pc, ah, argus, aris, ax.25, bbn-rcc-mon, bna, br-sat-mon, cbt, cftp, chaos compaq-peer, cphb, cpnx, crtp, crudp, dccp, dcn-meas, ddp, ddx, dgp, egp, eigrp emcon, encap, esp, etherip, fc, fire, ggp, gmtp, gre, hip, hmp, hopopt, i-nlsp, iatp icmp, idpr, idpr-cmtp, idrp, ifmp, igmp, igp, il, ip-in-ip, ipcomp, ipcu, ipip, iplt, ippc, iptm, ipv6, ipv6-frag, ipv6-icmp, ipv6-nonxt, ipv6-opts, ipv6-route, ipx-in-ip, irtp, iso-ip, iso-tp4, kryptolan, l2tp, larp, leaf-1, leaf-2, manet, merit-inp, mfe-nsp mhrp, micp, mobile, mobility header, mpls-in-ip, mtp, mux, narp, netblt, nsfnet-igp, nvp-ii ospf, pgm, pim, pipe, pnni, prm, ptp, pup, pvp, qnx, rdp, rohc, rsvp, rsvp-e2e-ignore, rvd, sat-expak, sat-mon, scc-sp, scps, sctp, sdrp, secure-vmtp, shim6, skip, sm, smp, snp, sprite-rpc sps, srp, sscopmce, st, stp, sun-nd, swipe, tcf, tcp, tlsp, trunk-1, trunk-2, ttp, udp, udplite uti, vines, visa, vmtp, vrrp, wb-expak, wb-mon, wesp, wsn, xnet, xns-idp,

Association de termes de recherche

Ces termes de recherche peuvent être associés dans des expressions plus complexes avec des mots-clés AND et OR. Par exemple, pour rechercher les paquets envoyés ou reçus sur 1.1.1.1 ou 2.2.2.2, entrez la chaîne suivante :

```
host 1.1.1.1 or host 2.2.2.2
```

Pour rechercher les paquets envoyés ou reçus sur 1.1.1.1 ou 2.2.2.2, entrez la chaîne suivante :

```
host 1.1.1.1 and host 2.2.2.2
```

Les associations liées à ces mots-clés sont conservées. Par exemple, pour la syntaxe suivante :

```
port 42 and host 1.1.1.1 or host 2.2.2.2
```

L'expression est évaluée ainsi :

- éléments envoyés ou reçus sur le port 42 et l'hôte 1.1.1.1 ou
- éléments envoyés ou reçus sur l'hôte 2.2.2.2, quels que soient les numéros de port

Vous pouvez changer l'association en utilisant des parenthèses, comme cela est présenté dans l'exemple suivant :

```
port 42 and (host 1.1.1.1 or host 2.2.2.2)
```

L'expression est évaluée afin de trouver les paquets envoyés du port 42 ou vers ce dernier ou envoyés de l'hôte 1.1.1.1 ou 2.2.2.2 ou vers ce dernier.

Concepts associés:

4, «Requêtes et recherches QRadar Network Packet Capture», à la page 19

5 Dispositifs QRadar Network Packet Capture regroupés

La fonction de regroupement IBM QRadar Network Packet Capture permet de regrouper plusieurs dispositifs physiques afin de former un seule entité logique pour l'administration et la recherche. En utilisant la fonction de regroupement, il est possible d'accéder à plusieurs taps réseau ainsi qu'à plusieurs dispositifs QRadar Network Packet Capture et de les utiliser comme s'il s'agissait d'un seul dispositif.

Un groupe QRadar Network Packet Capture peut capturer des données provenant de différents taps réseau. Vous devez configurer tous les dispositifs QRadar Network Packet Capture afin qu'ils puissent accéder à tous les membres de groupe QRadar Network Packet Capture sur l'interface réseau de gestion. De plus, le réseau doit disposer d'un serveur DNS.

Lorsque vous regroupez des dispositifs QRadar Network Packet Capture, vous pouvez rechercher toutes les données des membres de groupe à l'aide d'une seule requête de données. Le résultat de la recherche est un fichier PCAP qui contient les données fusionnées de tous les membres de groupe.

Pour accéder au groupe dans son intégralité, il vous suffit de vous connecter à un de ses membres. Une fois cette connexion établie, vous pouvez communiquer par proxy avec tous les autres membres du groupe QRadar Network Packet Capture.

La fonctionnalité de proxy est principalement conçue pour l'administration, la configuration et le débogage des dispositifs distants. Si une recherche qui concerne l'ensemble du groupe est lancée en utilisant le proxy et que l'utilisateur se trouve sur une instance QRadar Network Packet Capture distante, une quantité importante de trafic redondant est transmise via le réseau de gestion. Cela a des conséquences sur les performances d'extraction, selon la bande passante et le temps d'attente du réseau de gestion. Par conséquent, toute recherche effectuée sur un groupe QRadar Network Packet Capture doit toujours être lancée sur la machine principale ou locale, sans concentrateur ou proxy.

Concepts associés:

4, «Requêtes et recherches QRadar Network Packet Capture», à la page 19

Accès à un groupe

Certaines fonctionnalités se comportent différemment lorsque vous accédez à un dispositif IBM QRadar Network Packet Capture se trouvant dans un groupe.

Les dispositifs regroupés diffèrent des façons suivantes :

- Dans le widget GROUP VIEW de l'onglet DASHBOARD, plusieurs dispositifs QRadar Network Packet Capture (rassemblés dans un groupe) sont visibles.
- Le bouton **Switch To** correspond au changement de dispositif dans le widget GROUP VIEW de l'onglet DASHBOARD.
- Lorsque vous modifiez les comptes utilisateur et configurez Active Directory, les mises à jour sont automatiquement répercutées dans tous les membres de groupe.

Création et modification de groupe

Groupe d'homologues initial

Une demande de regroupement est lancée sur tout dispositif IBM QRadar Network Packet Capture, soit via l'interface graphique utilisateur, soit via l'API REST.

© Copyright IBM Corp. 2016, 2018

Dans l'exemple suivant, le dispositif QRadar Network Packet Capture qui demande la formation d'un groupe est appelé Dispositif A. Le dispositif récepteur de la demande de regroupement est appelé Dispositif B.

Par exemple, un groupe QRadar Network Packet Capture est formé de deux membres. Les événements suivants surviennent :

- Lors de la demande de regroupement, un nom d'utilisateur et un mot de passe ayant des droits d'accès de niveau administrateur doivent être fournis pour le dispositif B.
- La liste des comptes locaux et des configurations Active Directory est exportée du dispositif A dans le dispositif B. Toutes les configurations précédentes des comptes et d'Active Directory sur le dispositif sont remplacées.
- Toutes les données de capture sont conservées sur le dispositif A ainsi que sur le dispositif B et peuvent être recherchées à partir d'un des dispositifs.

Inclusion dans un groupe existant

La demande d'un dispositif QRadar Network Packet Capture autonome à inclure dans un groupe existant peut être lancée sur le dispositif autonome ou un membre du groupe. Dans l'exemple suivant, le dispositif QRadar Network Packet Capture autonome à inclure dans le groupe est appelé Dispositif C.

Par exemple, lorsqu'un dispositif QRadar Network Packet Capture est inclus dans un groupe existant :

- Les comptes locaux et les configurations Active Directory du groupe sont exportés dans le dispositif C. Le compte précédent et la configuration Active Directory sur le dispositif C sont remplacés.

Sortie d'un groupe

Les comptes locaux et la configuration Active Directory sont conservés en tant qu'instantané de l'état lorsqu'un dispositif QRadar Network Packet Capture est retiré d'un groupe. Aucune synchronisation avec le groupe supplémentaire n'a lieu.

Configuration d'un groupe QRadar Network Packet Capture

Configurez plusieurs dispositifs QRadar Network Packet Capture dans un groupe.

Avant de commencer

- Pour obtenir une description détaillée du regroupement de dispositifs IBM QRadar Network Packet Capture, voir Dispositifs QRadar Network Packet Capture regroupés.
- Vous êtes connecté au dispositif QRadar Network Packet Capture en tant qu'administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez effectuer la recherche dans l'ensemble du groupe, dans les membres sélectionnés ou dans un seul membre. Le résultat de la recherche est disponible dans un flux fusionné dans l'ordre chronologique. Chaque paquet est annoté avec l'UUID d'unité source et le port de réception au format PCAP/NG.

Procédure

1. Cliquez sur l'onglet **ADMIN** puis accédez au widget GROUP MEMBERSHIP.
2. Entrez l'adresse DNS ou IP du dispositif QRadar Network Packet Capture distant.
3. Entrez les informations de connexion d'un administrateur sur le dispositif QRadar Network Packet Capture distant.
4. Cliquez sur **Add Host**.

Résultats

Le dispositif QRadar Network Packet Capture distant est placé dans le même groupe que le dispositif auquel vous êtes connecté.

Que faire ensuite

Cliquez sur **Remove** pour retirer un dispositif QRadar Network Packet Capture du groupe.

6 Empilage QRadar Network Packet Capture

Vous pouvez étendre le stockage disponible pour capturer des données en connectant plusieurs dispositifs IBM QRadar Network Packet Capture ensemble dans une topologie en anneau pour créer une pile.

La pile permet de répartir les données de capture entre les différents dispositifs connectés. Elle peut connecter jusqu'à 16 dispositifs, mais semble être une entité unique qui capture les données d'un TAP d'un port 10 Gbits unique et se comporte comme telle.

Contrôleur de pile
Le contrôleur de pile est le dispositif qui reçoit le trafic surveillé, également appelé "point TAP". Le contrôleur de pile gère la configuration globale pour la pile. Il ne peut donc y avoir qu'un seul contrôleur dans chaque pile.

Noeud de pile
Le noeud de pile est le dispositif utilisé comme stockage des données de capture. Vous pouvez disposer de 15 noeuds dans une pile.

Avantages des dispositifs d'empilage

L'empilage permet de faire évoluer le stockage et d'étendre le délai de conservation des données de capture.

Lorsque la pile capture activement les données, vous pouvez effectuer les actions suivantes :

- Mettez une pile hors ligne, mettez-la à niveau et réinsérez-la dans la pile.

  Remarque : Cette possibilité ne concerne pas le contrôleur de pile.
- Ajoutez un dispositif pour étendre la capacité d'une pile.

  Le matériel et la taille de stockage des dispositifs peut varier. Tout le stockage disponible dans la pile est utilisé pour la capture des données.

Stockage des données

La topologie en anneau de la pile permet de protéger les données de capture. Les données de capture sont stockées dans la pile par délai, c'està-dire qu'un dispositif contient toutes les données de capture pour un certain délai et remplace les anciennes données.

L'intervalle de temps pour la totalité de la pile est établi par concaténation de tous les dispositifs, dans l'ordre. Par exemple, dans une pile qui comporte trois dispositifs, le dispositif A stocke les données du délai 0 à 9, le dispositif B stocke les données du délai 10 à 19 et le dispositif C stocke les données du délai 20 à 29. A mesure que les dispositifs se remplissent de données, ce sont les plus anciennes données de capture qui sont remplacées en premier. Le dispositif A stocke maintenant les données du délai 30 à 39, en remplaçant les données du délai 0 à 9.

Si un dispositif est mis hors ligne, il se produit un vide dans les données de capture, mais ce vide est limité au délai pour lequel les données sont contenues sur le dispositif hors ligne. Dans l'exemple de pile, si le dispositif B est hors ligne, les données du délai 10 à 19 ne sont pas disponibles, mais toutes les autres données de capture de la pile sont disponibles.

© Copyright IBM Corp. 2016, 2018

Considérations relatives aux performances

La topologie en anneau utilisée pour connecter les dispositifs IBM QRadar Network Packet Capture empilés est conçue pour obtenir une haute disponibilité pour la capture continue des données.

Chaque paquet transmis entre les dispositifs comporte des données supplémentaires sur le statut de la pile. Par exemple, les paquets IP incluent des informations, comme le noeud de la pile qui stocke les données et le statut des noeuds de pile, et surveillent la connectivité entre les dispositifs. En fonction de votre environnement, les données supplémentaires transmises avec chaque paquet peuvent aboutir à des performances de capture inférieures à 10 Gbits/s dans certaines circonstances.

Par exemple, le trafic réseau qui comprend une proportion élevée de petits paquets dans le temps peut aboutir à un taux de capture inférieur. Alors que cette situation n'est pas typique pour la plupart des déploiements, si dans ces circonstances, votre déploiement nécessite une capture entière de 10 GBits/s, il est recommande de déployer des dispositifs QRadar Network Packet Capture comme dispositifs autonomes au lieu d'utiliser une pile.

Création d'une pile

Créez une autre pile physique QRadar Network Packet Capture pour augmenter l'espace de stockage disponible pour vos données de capture.

Avant de commencer

Avant de créer la pile, préparez votre environnement.

- Vous pouvez empiler 16 dispositifs maximum, dont le contrôleur de pile. La distance maximale de câblage physique entre deux dispositifs est de 10 mètres.
- Assurez-vous que tous les dispositifs dans la pile exécutent la même version du logiciel QRadar Network Packet Capture.
- Assurez-vous que tous les dispositifs font partie d'un groupe. Pour plus d'informations, voir Dispositifs regroupés.
- Interconnectez les dispositifs pour former un anneau afin que tous les dispositifs puissent communiquer entre eux. Pour découvrir un exemple de schéma de câblage, voir Topologie de l'empilage.

  Remarque : Le routage et la commutation ne sont pas autorisés. Seules les connexions entre homologues sont autorisées.

Procédure

1. Sur le contrôleur de pile, connectez le port 2 au commutateur au port SPAN surveillé ; il s'agit du réseau TAP.
2. Facultatif : Sur le contrôleur de pile, connectez le port 3 à un dispositif QRadar QNI.

   Le port 3 est utilisé pour retransmettre toutes les données de capture au dispositif QNI. Les données sont retransmises dans un format spécial avec un horodatage de capture des données intégré dans le délai.
3. Sur es noeuds de pile, connectez le port 0 et le port 1 pour former un anneau.

   Remarque : Pour les noeuds de pile, les ports 2 et 3 ne doivent pas être utilisés.

Exemple

Le diagramme suivant présente un exemple de topologie constituée d'un contrôleur de pile (dispositif A) et de trois noeuds de pile (dispositifs B, C et P).

Les ports NT40E3-4 sont connectés en utilisant les ports 0 et 1 pour former un anneau.

1. Le port 0 du dispositif A se connecte au port 1 du dispositif B.
2. Le port 0 du dispositif B se connecte au port 1 du dispositif C.
3. Le port 0 du dispositif C se connecte au port 1 du dispositif A.

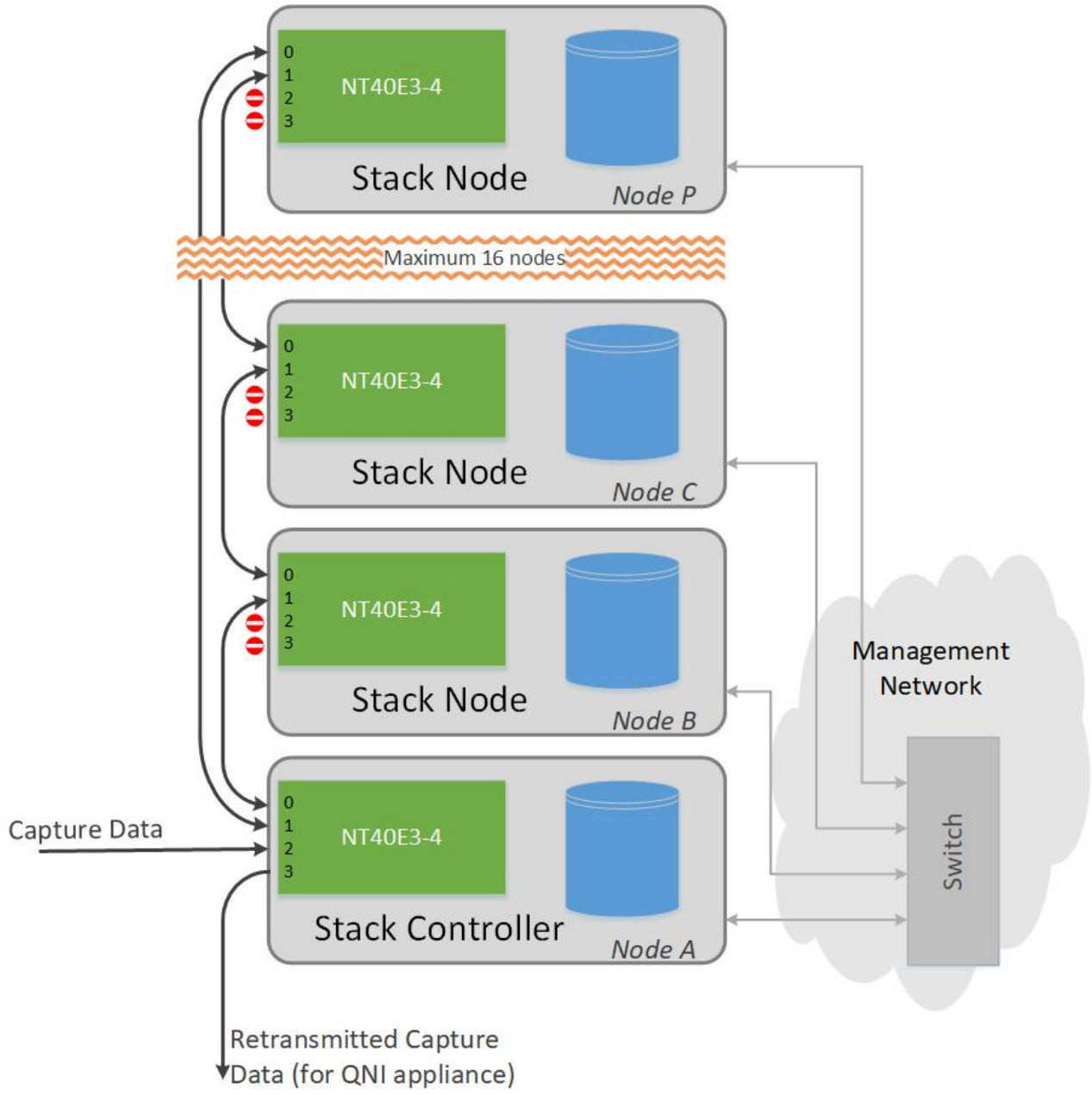


Figure 12. Exemple de topologie QRadar Network Packet Capture.

Configuration d'une pile

Utilisez le widget STACKING pour configurer la pile.

Avant de commencer

Si un dispositif contient des données de capture qui ne sont pas pertinentes pour la pile que vous y ajoutez, supprimez les données de capture du dispositif avant de les ajouter à la pile.

Pourquoi et quand exécuter cette tâche

Le widget STACKING affiche la configuration de la pile. L'image suivante présente une pile totalement configurée et en cours de capture de données :

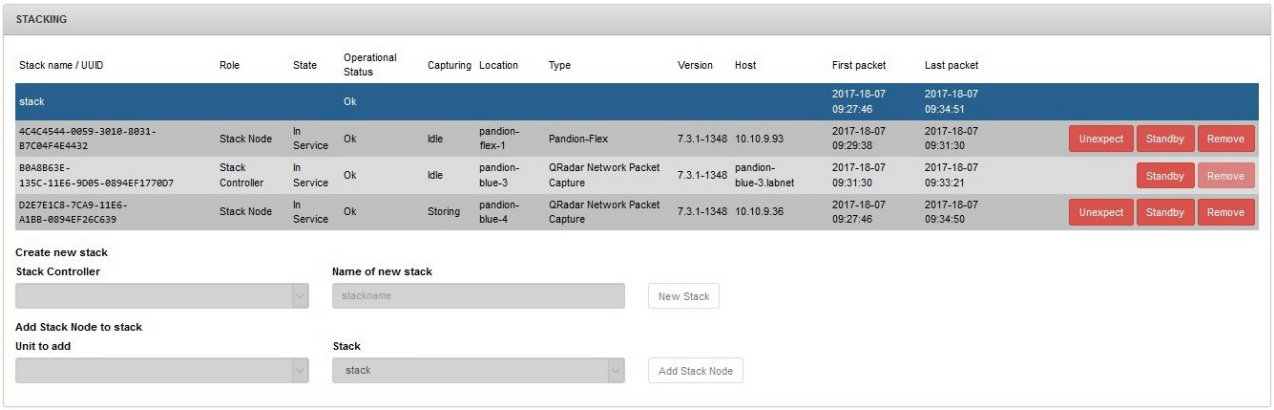


Figure 13. Configuration d'une pile.

Un seul dispositif à la fois capture des données. A mesure que le dispositif se remplit de données de capture, un autre dispositif de la pile devient le dispositif de **stockage**.

L'ordre d'activation des dispositifs pour la capture est aléatoire. L'ordre des dispositifs dans le widget STACKING ou le câblage physique peut avoir une influence sur la sélection des dispositifs. Cependant, lorsque tous les dispositifs de la pile contiennent des données de capture, le dispositif de capture suivant est toujours le dispositif qui contient les données de capture dont l'horodatage est le plus ancien.

Procédure

1. Cliquez sur l'onglet **ADMIN** et ouvrez le widget GROUP MEMBERSHIP. Vérifiez que tous les dispositifs de la pile sont regroupés correctement.
2. Affectez un contrôleur de pile et créez la pile comme suit :
   a. Dans le widget STACKING, dans la liste **Contrôleur de pile**, sélectionnez le dispositif que vous souhaitez définir comme contrôleur de pile.

      Le nom de la pile est utilisé pour identifier la pile de manière unique ; il est utilisé nulle part ailleurs dans la configuration.
   b. Dans la zone **Name of new stack**, entrez un nom descriptif pour le contrôleur de pile, puis cliquez sur **New Stack**.

      La pile est créée et s'affiche en tant que nouvelle entrée dans le widget STACKING.
3. Ajoutez les noeuds de pile à la pile :
   a. Dans la zone de liste **Unit to add**, sélectionnez le dispositif à ajouter à la pile.
   b. Dans la liste **Stack**, sélectionnez le nom de la pile à ajouter au dispositif et cliquez sur **Add Stack Node**.

      Si un groupe contient plusieurs piles, veillez à sélectionner dans le menu le nom de pile approprié.
   c. Répétez cette procédure pour chaque dispositif à ajouter à la pile.

      Une fois tous les dispositifs ajoutés, la pile doit s'afficher comme saine et prête à activer la capture de données.

Remarque : Lorsque vous ajoutez des noeuds de pile, le statut opérationnel du widget STACKING peut afficher des erreurs de statut opérationnel temporaires. Ces erreurs proviennent du fait que la connectivité dans l'anneau de la pile est incomplète tant que tous les noeuds de pile n'ont pas été ajoutés.

4. Vérifiez la configuration de la pile :
   a. Sélectionnez la pile et vérifiez que la liste de dispositifs est telle qu'attendue pour la pile.
   b. Vérifiez que chaque dispositif de la pile a le même numéro de version et affiche les valeurs suivantes :
      - Operational Status = OK
      - State = In Service

      Vous êtes maintenant prêt à activer la capture de données.
5. Activez la capture des données :
   a. Cliquez sur **Expect** en regard de chaque noeud de pile de la pile pour activer le dispositif pour la capture de données.

      Remarque : Par défaut, tous les noeuds de pile sont définis sur **Unexpect** lorsqu'ils viennent d'être ajoutés à la pile afin d'empêcher le dispositif de stocker des données capturées tant qu'il n'est pas physiquement activé.
   b. Accédez au widget **GROUP MEMBERSHIP** et cliquez sur **Switch to** pour le contrôleur de pile approprié.
   c. Accédez à **Traffic Capture** et cliquez sur **Traffic Capture** pour commencer à capturer des données.
   d. Cliquez sur l'onglet DASHBOARD du contrôleur de pile pour vérifier le trafic entrant.

      Le port 2 du contrôleur de pile est le port réseau TAP de la pile. Si du trafic est entrant sur ce port, vous voyez que :

      1) Le modèle de trafic correspond au trafic entrant.
      2) Le modèle de trafic sur le tableau de bord du contrôleur de pile de tous les noeuds de la pile est deux fois plus grand que le trafic entrant (plus un certain nombre de paquets monodiffusion 64-127 octets).

         Remarque : Le trafic entrant est transmis à tous les dispositifs de la pile, dans les deux directions (dans le sens des aiguilles d'une montre et dans le sens contraire) sur les ports 0 et 1. Dans le même temps, un protocole de pile propriétaire, qui transporte en continu de petites trames sur l'anneau, est exécuté.
6. Vérifiez les données de capture dans le widget STACKING comme suit :
   a. Vérifiez les dispositifs de votre pile et recherchez ceux dont la colonne **Capturing** affiche la valeur **Storing**.

      Un seul dispositif à la fois capture les données, donc un seul dispositif affiche **Storing**, tandis que les autres dispositifs sont inactifs.
   b. Sur ce dispositif, vérifiez que les colonnes **First packet**et **Last packet** affichent des valeurs d'horodatage valides.

      A mesure que le dispositif se remplit de données de capture, un autre dispositif de la pile devient le dispositif de stockage et les horodatages des colonnes First packet et Last packet du nouveau dispositif sont mises à jour.

Ajout d'un dispositif à une pile active

Vous pouvez étendre la capacité d'une pile en ajoutant des dispositifs alors que la pile est en train de capturer des données.

Procédure

1. Installez un dispositif QRadar Network Packet Capture de même version de logiciel que le dispositif présent dans la pile que vous voulez étendre.
2. Effectuez l'installation physique du dispositif.

   Cette procédure inclut la connexion du dispositif au réseau de gestion commun, en rompant l'anneau de la pile et en connectant le nouveau dispositif à l'anneau. Vous pouvez installer le nouveau dispositif dans n'importe quel emplacement physique de la pile. Pour plus d'informations, voir «Création d'une pile», à la page 32.

   Remarque : Pendant cette procédure, la connectivité dans l'anneau de la pile est incomplète et le statut opérationnel du widget STACKING peut afficher des erreurs de câblage temporaires.
3. Incluez le nouveau dispositif dans le groupe et ajoutez-le à la pile, comme indiqué à l'étape 3, Ajout d'un noeud de pile.
4. Vérifiez le widget STACKING pour prendre connaissance du statut du nouveau dispositif.

   Le dispositif est totalement opérationnel lorsque **Operational Status** est défini sur **OK**, les paramètres**First packet** et **Last packet** sont définis sur **N/A** et il ne reste aucune erreur de câblage.

   Lorsque le dispositif qui capture des données est saturé, la pile passe au nouveau dispositif inséré pour la capture des données.

Retrait d'un dispositif d'une pile

Lorsque vous supprimez un dispositif de la pile, les données de capture sur le dispositif sont conservées. Vous pouvez exécuter des recherches locales sur le dispositif pour accéder aux données.

Procédure

Pour supprimer définitivement un dispositif d'une pile, sélectionnez le dispositif et cliquez sur **Supprimer** dans le widget STACKING.

Remarque : Vous ne pouvez pas supprimer le contrôleur de pile tant que tous les noeuds de pile n'ont pas été supprimés de la pile.

Que faire ensuite

Retirez physiquement le câblage du dispositif et reconnectez l'anneau de la pile. Des erreurs de câblage temporaires peuvent s'afficher lorsque la connectivité de la pile est rétablie.

Conservation des noeuds de pile existants

Vous pouvez placer un noeud de pile en mode veille pour permettre les mises à niveau et la maintenance alors que le reste de la pile est actif. Grâce à cette fonction, vous pouvez mettre à niveau chacun de vos noeuds de pile, tandis que les dispositifs en service continuent à capturer des données.

Avant que vous puissiez mettre à jour le contrôleur de pile, vous devez désactiver la capture des données et mettre la pile entière hors ligne.

Avant de commencer

Vérifiez que tous les noeuds de la pile ont été mis à jour avant de mettre à jour le contrôleur de pile.

Pourquoi et quand exécuter cette tâche

Lorsqu'un dispositif est en mode veille, vous pouvez mettre à jour le système d'exploitation et le logiciel d'application du dispositif. S'il n'est pas nécessaire de redémarrer le dispositif, la connectivité entre le

dispositif et l'anneau de la pile est conservée. Si le dispositif capture des données alors que le mode veille est activé, la pile transfère immédiatement la capture active à un autre dispositif.

Si une mise à jour concerne les communications avec le contrôleur de pile, par exemple, une mise à jour des protocoles, les noeuds de pile peuvent gérer cette opération pendant la procédure de mise à jour, car ils sont rétrocompatibles avec les protocoles et les commandes exécutées à partir du contrôleur de pile.

Un noeud de pile en mode veille possède les caractéristiques suivantes :

- Il continue à apparaître dans la liste de piles dans le widget STACKING.
- Il conserve la connectivité de l'anneau de la pile.
- Il conserve l'appartenance au groupe.
- Il inclut les données de capture dans les recherches.
- Il n'est pas utilisé comme dispositif de capture active dans la pile. Les nouvelles données ne sont pas capturées par ce dispositif.

Vous ne pouvez pas placer le contrôleur de pile en mode veille sans interruption de service, car c'est le seul dispositif qui possède un port TAP et il distribue les données à tous les dispositifs de la pile.

Procédure

1. Dans le widget STACKING, sélectionnez le dispositif à utiliser, puis cliquez sur **Standby**.

   Remarque : Pour autoriser le délai maximal pour appliquer des mises à jour au dispositif, sélectionnez le noeud de pile possédant l'horodatage du **premier paquet** et du **dernier paquet**, mais qui ne capture pas de données actuellement.
2. Appliquez les mises à jour au dispositif de veille.
3. Dans le widget STACKING, lorsque la maintenance est terminée, sélectionnez le dispositif, puis cliquez sur **In Service** pour le réactiver.

7 Identification et résolution des problèmes - Voyants externes

Utilisez l'état et la couleur des voyants externes pour faciliter l'identification et la résolution des problèmes de votre dispositif IBM QRadar Network Packet Capture.

Les informations contenues dans l'image et les tableaux suivants identifient l'emplacement des différents voyants externes et permettent de résoudre les problèmes.

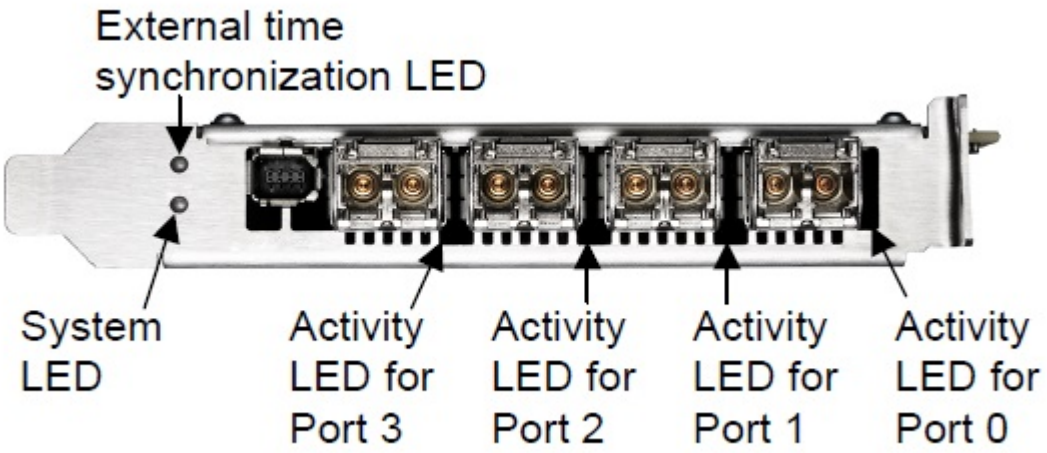


Figure 14. Emplacement des voyants externes

Voyants d'activité

Le tableau ci-dessous décrit les états standard indiqués par la couleur des voyants d'activité.

Tableau 4. Voyants d'activité et statut de fonctionnement du dispositif

Etat et couleur	**Condition**
Eteint	Le pilote n'est pas chargé, la liaison Ethernet est inactive ou le port est déconnecté.
Témoin vert allumé en continu	Le pilote est chargé et la liaison Ethernet est opérationnelle mais il n'existe aucun trafic.
Vert clignotant	Le pilote est chargé mais il existe du trafic sur la liaison Ethernet.

Voyant système

Le tableau ci-dessous décrit les états standard indiqués par la couleur du voyant système.

Tableau 5. Voyant système et statut de fonctionnement du dispositif

Etat et couleur	**Condition**
Eteint	L'alimentation est coupée.
Rouge continu	Lors du démarrage et lorsque l'appareil est sous tension, l'accélérateur vérifie les alimentations électriques.

© Copyright IBM Corp. 2016, 2018

Tableau 5. Voyant système et statut de fonctionnement du dispositif (suite)

Etat et couleur	Condition
Rouge clignotant	Après le démarrage et la mise sous tension, une erreur matérielle irrécupérable se produit.
Jaune continu	Lors du démarrage et lorsque l'appareil est sous tension, les alimentations électriques fonctionnent.
Jaune clignotant	Il existe une nouvelle entrée dans le journal matériel.
Vert continu	L'élément FPGA est chargé et le système est en cours d'exécution.

Voyant de synchronisation d'horloge externe

Le tableau ci-dessous décrit les états standard indiqués par la couleur du voyant de synchronisation d'horloge externe.

Tableau 6. Voyant de synchronisation d'horloge externe et le statut de fonctionnement du dispositif

Etat et couleur	Condition
Eteint	Aucun pilote n'est chargé ou la liaison Ethernet sur le port PTP (Precision Time Protocol) est inactive.
Jaune continu	La liaison Ethernet sur le port PTP est active.

Remarques

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. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service 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
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

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, Japan

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 tacites, 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.

Toute référence à ces informations sur des sites web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites web. Les documents sur ces sites web ne font pas partie des documents de ce produit IBM et l'utilisation de ces sites web se fait à vos propres risques.

© Copyright IBM Corp. 2016, 2018

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.

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
U.S.A.

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'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

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 un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

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. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produit et de service peuvent être des marques d'IBM ou d'autres sociétés. 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.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site web IBM.

Utilisation personnelle

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

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 pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite 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. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. 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 en ligne

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. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

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 à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et la section "Cookies, pixels espions et autres technologies" de la

Déclaration IBM de confidentialité sur Internet sur le site http://www.ibm.com/privacy/details/fr/fr, ainsi que la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site http://www.ibm.com/software/info/product-privacy (en anglais).