IBM Security QRadar - Guide d'utilisation des sources de journal

QRadar SIEM 7.2.0

Mai 2013

DO05082013-A

Note: Avant d'utiliser ces informations et le produit associé, prenez connaissance des informations figurant à la section “Avis et marques” sur page 122.

SOMMAIRE

C CONFIGURATION DU MODÈLE DCOM

D AVIS ET MARQUES

INDEX

A PROPOS DE CE GUIDE

Le document *IBM Security QRadar - Guide d'utilisation des sources de journal* fournit des informations relatives à la configuration des sources de journal et des protocoles associés dans QRadar.

Les sources de journal vous permettent d'intégrer des événements et des journaux à partir d'unités externes (Device Support Modules (DSM)) avec QRadar et QRadar Log Manager. Sauf indication contraire, toutes les références à QRadar dans ce document peuvent concerner les produits suivants :

- IBM Security QRadar SIEM
- IBM Security QRadar Log Manager

Utilisateurs concernés

Ce guide est destiné à l'administrateur système responsable de la configuration de IBM Security QRadar sur votre réseau. Ce guide suppose que vous disposez d'un accès en tant qu'administrateur à QRadar et que vous maîtrisez votre réseau d'entreprise et les technologies de mise en réseau.

Conventions

Les conventions suivantes sont utilisées dans ce guide :

Remarque : Indique que les informations fournies viennent compléter la fonction ou l'instruction associée.

ATTENTION : *Indique que les informations sont capitales. Une mise en garde vous avertit de l'éventuelle perte de données ou d'un éventuel endommagement de l'application, du système, d'une unité ou d'un réseau.*

AVERTISSEMENT : *Indique que les informations sont capitales. Un avertissement vous alerte de dangers, menaces ou risques de blessure potentiels. Prenez connaissance de tous les avertissements avant de poursuivre.*

Documentation technique

Pour accéder à davantage de documentation technique, de notes techniques et des notes sur l'édition, voir la documentation ***Note technique sur l'accès à la documentation QRadar IBM Security.*** (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacter le service clients

Pour plus d'informations sur la façon de contacter le service clients, voir le document ***Note technique sur le support et le téléchargement***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

Déclaration de pratiques recommandées de sécurité

La sécurité système IT implique la protection des systèmes et des informations à travers la prévention, la détection et la réponse aux accès incorrects à l'intérieur ou à l'extérieur de votre entreprise. L'accès incorrect peut aboutir à des informations modifiées, détruites, non appropriées ou mal utilisées ; il peut également entraîner des dommages ou une utilisation inappropriée de vos systèmes, notamment pour attaquer d'autres systèmes. Aucun système ou produit ne doit être considéré comme étant complètement sécurisé et aucun produit, service ou mesure de sécurité ne peut être complètement efficace dans la prévention de l'utilisation ou l'accès incorrects. Les systèmes, produits et servies IBM sont conçus pour faire partie d'une approche de sécurité complète qui impliquera nécessairement des procédures opérationnelles supplémentaires et peut requérir d'autres systèmes, produits et services afin d'être le plus efficace possible. IBM NE GARANTIT PAS QUE CES SYSTEMES, PRODUITS OU SERVICES SONT A L'ABRI OU METTRONT VOTRE ENTREPRISE A L'ABRI DE L'ACTION MALVEILLANTE OU ILLEGALE DE N'IMPORTE QUELLE PARTIE.

1 GESTION DES SOURCES DE JOURNAUX

Vous pouvez configurer IBM Security QRadar ou IBM Security QRadar Log Manager pour consigner et corréler les événements reçus à partir de sources externes tels qu'un équipement de sécurité (par exemple, pare-feux et IDS) et un équipement de réseau (par exemple, des commutateurs et des routeurs).

Les sources de journal vous permettent d'intégrer QRadar ou QRadar Log Manager avec ces périphériques externes. Sauf indication contraire, toutes les références à QRadar dans le guide se réfèrent à la fois à QRadar et QRadar Log Manager.

Remarque : Les informations disponibles dans cette documentation sont basées sur les fichiers RPM les plus récents qui se trouvent sur le site Web IBM à l'adresse *http://www.ibm.com/support*.

Cette section fournit des informations les éléments suivants :

- **Configuration de QRadar pour recevoir des événements**
- **Gestion de sources de journal**
- **Lorsque vous sélectionnez le type de source de journal dans la zone de liste Log Source Type, les options du protocole pour la source de journal sélectionnée s'affichent dans la zone de liste Protocol Configuration.**
- **Sources de journal groupées**
- **Définition de l'ordre d'analyse syntaxique de la source de journal**

Configuration de QRadar pour recevoir des événements

QRadar reconnaît automatiquement plusieurs sources de journal dans votre déploiement qui envoient des messages syslog.

Toutes les sources de journal qui sont automatiquement reconnues par QRadar apparaissent dans la fenêtre Log Sources. Vous pouvez configurer automatiquement les sources de journal reconnues selon le collecteur d'événements à l'aide du paramètre Autodetection Enabled dans la configuration du collecteur d'événement. Pour plus d'informations, voir *IBM Security QRadar Administration Guide en utilisant l'éditeur de déploiement.*

Remarque : Pour plus d'informations sur les sources de journal reconnues automatiquement et sur les configurations spécifiques à votre périphérique ou appareil, voir le *IBM Security QRadar Guide de configuration DSM*.

Pour configurer QRadar afin de recevoir des événements sur les périphériques :

Etape 1 Configurez le DSM (Device Support Module) externe pour envoyer des événements vers QRadar.

Pour obtenir des informations sur la configuration des DSM, voir *IBM Security QRadarConfiguring DSMs Guide* et la documentation de votre fournisseur.

Etape 2 Configurez les sources de journal dansQRadar pour recevoir les sur les DSM. Voir **Gestion de sources de journal**

Remarque : Vous devez disposer de privilèges administratives pour configurer les sources de journal dans QRadar. Pour obtenir des informations sur l'accès à l'onglet **Admin**, voir *IBM Security QRadar Administration Guide*.

Gestion de sources de journal

Une source de journal fournit des événements sur votre déploiement via les DSM. En utilisant l'onglet **Admin**, vous pouvez :

- Afficher les sources de journal. Voir **Affichage de sources de journal**.
- Ajouter une source de journal. Voir **Ajout d'une source de journal**.
- Editer une source de journal existante. Voir **Edition d'une source de journal**.
- Activer ou désactiver une source de journal. Voir **Activation ou désactivation d'une source de journal**.
- Supprimer une source de journal. Voir **Suppression d'une source de journal**.
- Ajouter un groupe de source de journal. Voir **Ajout de plusieurs sources de journal**.
- Editer un groupe de source de journal. Voir **Edition de plusieurs sources de journal**.

Affichage de sources de journal

Vous pouvez afficher des sources de journal existantes pour déterminer les journaux d'événements qui sont collectées à partir de vos appareils réseau.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Si une source de journal n'a reçu aucun événement dans le délai de time-out syslog configuré, la colonne Status affiche Error. Si vous configurez manuellement une source de journal qui utilise syslog, la colonne syslog affiche un statut d'erreur jusqu'à ce que cette source de journal reçoive un événement.
Pour plus d'informations sur le paramètre Syslog Event Timeout, voir *IBM Security QRadar Administration Guide*.

Remarque : Les sources de journal ajoutées en vrac affichent N/A dans la colonne **Status**.

Ajout d'une source de journal

Vous ajoutez une source de journal à votre déploiement pour permettre à QRadar de recevoir des journaux d'événement à partir de votre périphérique ou appareil réseau.

La plupart des périphériques de votre réseau peuvent nécessiter des paramètres de configuration spécifiques. Les étapes spécifiques de la configuration de votre périphérique peuvent être consultées dans le in the *IBM Security QRadar Guide de configuration DSM*.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Cliquez sur **Add**.

Etape 5 Saisissez les valeurs pour les paramètres suivants :

Tableau 1-1 Paramètres de source de journal génériques

Paramètre	Description
Log Source Name	Saisissez un nom approprié de la source de journal. Le nom peut contenir jusqu'à 225 caractères.
Log Source Description	Saisissez une description pour la source de journal (facultatif).
Log Source Type	Dans la zone de liste, sélectionnez le type de source de journal à ajouter.
Protocol Configuration	Dans la zone de liste, sélectionnez la configuration du protocole pour la source de journal. La configuration du protocole vous permet de définir les paramètres pour la communication avec la source de journal tels que les protocoles spécifiques JDBC, syslog, SNMP ou fournisseur. Les protocoles disponibles affichés dans la zone de liste de protocoles de configuration sont basés sur le type de source de journal sélectionné. Pour plus d'informations sur les protocoles et paramètres spécifiques, voir **Lorsque vous sélectionnez le type de source de journal dans la zone de liste Log Source Type, les options du protocole pour la source de journal sélectionnée s'affichent dans la zone de liste Protocol Configuration.**.

Tableau 1-1 Paramètres de source de journal génériques (suite)

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP ou un nom d'hôte pour identifier la source de journal. L'adresse de l'identifiant doit être le périphérique source qui génère l'événement. Par exemple, si votre réseau contient plusieurs périphériques et une console de gestion, vous devez spécifier l'adresse IP du périphérique individuel dans le champ Log Source Identifier. Cela permet aux événements transférés vers QRadar de contenir l'adresse IP ou le nom d'hôte de la source d'événement, au lieu de la console de gestion.
Enabled	Sélectionnez cette case pour activer la source de journal. Par défaut, la case est cochée.
Credibility	Dans la zone de liste, sélectionnez la crédibilité de la source de journal. L'intervalle est compris entre 0 et 10. La crédibilité indique l'intégrité d'un événement ou attaque tel que déterminé par le classement de crédibilité à partir des périphériques sources. La crédibilité augmente si plusieurs sources rapportent le même événement. La valeur par défaut est de 5.
Target Event Collector	Dans la zone de liste, sélectionnez le collecteur d'événement à utiliser en tant que cible pour la source de journal.
Coalescing Events	Cochez cette case pour autoriser la coalescence (regroupement) d'événements. Les sources de journal reconnues automatiquement utilisent la valeur par défaut configurée dans le menu déroulant **Coalescing Events** dans la fenêtre QRadar Settings sur l'onglet **Admin**. Cependant, lorsque vous créez une nouvelle source de journal ou mettez à jour la configuration pour reconnaître automatiquement la source de journal, vous pouvez redéfinir la valeur par défaut en configurant cette case pour chaque source de journal. Pour plus d'informations sur les paramètres, voir *IBM Security QRadar Administration Guide*.
Store Event Payload	Sélectionnez la case pour activer ou désactiver QRadar du stockage de la charge utile d'événement. Les sources de journal reconnues automatiquement utilisent la valeur par défaut du menu déroulant **Store Event Payload** dans la fenêtre QRadar Settings sur l'onglet **Admin**. Cependant, lorsque vous créez une nouvelle source de journal ou mettez à jour la configuration pour reconnaître automatiquement la source de journal, vous pouvez redéfinir la valeur par défaut en configurant cette case pour chaque source de journal. Pour plus d'informations sur les paramètres, voir le Guide d'administration *IBM Security QRadar*.

Tableau 1-1 Paramètres de source de journal génériques (suite)

Paramètre	Description
Log Source Extension	Le paramètre Log Source Extension ne s'affiche que si vous disposez d'une extension de source de journal dans votre déploiement. Les extensions de source de journal vous permettent d'étendre immédiatement les routines d'analyse de sources de journal spécifiques, qui garantissent que les DSM envoient des données valides à QRadar. Pour plus d'informations sur les extensions de la source de journal, voir **Gérer des extensions de source de journal**. Dans la zone de liste, sélectionnez l'extension de source de journal à utiliser pour cette source de journal.
Groupes	Sélectionnez un ou plusieurs groupes pour la source de journal.

Etape 6 Cliquez sur **Save**.

Etape 7 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Edition d'une source de journal

Vous pouvez éditer une source de journal afin de mettre à jour les paramètres de configuration.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Sélectionnez la source de journal à éditer.

Remarque : Pour modifier le nom, la description, l'identificateur ou le groupe de la source de journal, cliquez deux fois sur la source de journal.

Etape 5 Cliquez sur **Edit**.

Etape 6 Configurez les valeurs pour votre source de journal tel que décrit dans **Tableau 1-1**.

Etape 7 Cliquez sur **Save**.

Les modifications sont immédiatement enregistrées pour votre source de journal.

Activation ou désactivation d'une source de journal

Vous pouvez activer ou désactiver une source de journal dans QRadar.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Sélectionnez la source de journal à activer ou à désactiver.

Etape 5 Cliquez sur **Enable/Disable**.

Lorsqu'une source de journal est activée, la colonne Enabled indique true. Lorsqu'une source de journal est désactivée, la colonne **Status** indique **Disabled**.

Les sources de journal désactivées ne sont pas prises en compte dans la limite de votre licence de source de journal dans QRadar. Cependant, Si vous ne parvenez pas à activer une source de journal, cela signifie que vous avez dépassé les restrictions de votre licence. Pour plus d'informations sur vos limites de licence, voir la section Gestion du système du document *IBM Security QRadar - Guide d'administration*. Si vous exigez des limites de licence supplémentaires, contactez votre commercial.

Suppression d'une source de journal

Vous pouvez supprimer une source de journal à partir de QRadar.

Si vous supprimez une source de journal, l'opération ne supprime pas les données de source de journal stockées ; cependant, les index des données sont supprimées et peuvent rendre difficile la recherche de données de source de journal.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Sélectionnez la source de journal à supprimer.

Etape 5 Cliquez sur **Delete**.

Etape 6 Cliquez sur **OK**.

Remarque : Vous pouvez supprimer plusieurs sources de journal en maintenant appuyée la touche majuscule pour sélectionner plusieurs sources de journal et cliquer sur **Delete**.

Ajout de plusieurs sources de journal

Vous pouvez ajouter plusieurs sources de journal à QRadar pour partager un protocole de configuration.

Les sources de journal vous permettent de regrouper, d'ajouter et de configurer des hôtes en téléchargeant un fichier texte, à l'aide d'une analyse de domaine ou en entrant un nom d'hôte ou une adresse IP. Un nombre maximal de 500 hôtes actifs ou d'adresses IP peut partager une configuration de protocole unique. Si vous tentez d'ajouter plus de 500 hôtes, un message d'erreur s'affiche.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 A l'aide la zone de liste **Bulk Actions,** sélectionnez **Bulk Add**.

Etape 5 Entrez les valeurs des paramètres, si nécessaire :

Tableau 1-2 Ajout de paramètres de source de journal en vrac

Paramètre	Description
Bulk Log Source Name	Entrez ce nom qui convient au groupe de source de journal bulk. Le nom peut contenir jusqu'à 225 caractères. ***Remarque :*** *L'ajout automatique d'une source de journal bulk crée un groupe de source de journal à l'aide du nom que vous avez entré dans ce champ.*
Log Source Type	Dans la zone de liste, sélectionnez le type de source de journal à ajouter.
Protocol Configuration	Dans la zone de liste, sélectionnez le protocole à utiliser pour cette source de journal. Seuls les protocoles disponibles pour le type de source de journal sélectionné s'affichent dans la liste. Les paramètres de configuration requises apparaissent. Pour plus d'informations sur les paramètres du protocole, voir **Lorsque vous sélectionnez le type de source de journal dans la zone de liste Log Source Type, les options du protocole pour la source de journal sélectionnée s'affichent dans la zone de liste Protocol Configuration.**.
Enabled	Sélectionnez cette case pour activer la source de journal. Par défaut, la case est cochée.
Credibility	Dans la zone de liste, sélectionnez la crédibilité du log source Bulk. L'intervalle est compris compris entre 0 et 10. La crédibilité indique l'intégrité d'un événement ou attaque tel que déterminé par le classement de crédibilité à partir des périphériques sources. La crédibilité augmente si plusieurs sources rapportent le même événement. La valeur par défaut est de 5.
Target Event Collector	Dans la zone de liste, sélectionnez le collecteur d'événement à utiliser en tant que cible pour la source de journal.
Coalescing Events	Cochez cette case pour autoriser la coalescence (regroupement) d'événements. Les sources de journal automatiquement découvertes utilisent la valeur configurée par défaut dans la zone de liste **Coalescing Events** dans la fenêtre QRadar Settings sur l'onglet **Admin** Cependant, lorsque vous créez une nouvelle source de journal ou mettez à jour la configuration pour reconnaître automatiquement la source de journal, vous pouvez redéfinir la valeur par défaut en configurant cette case pour chaque source de journal. Pour plus d'informations sur les paramètres, voir le Guide d'administration *IBM Security QRadar*.

Tableau 1-2 Ajout de paramètres de source de journal en vrac (suite)

Paramètre	Description
Store Event Payload	Sélectionnez la case pour activer ou désactiver QRadar du stockage de la charge utile d'événement. Les sources de journal automatiquement reconnues utilisent la valeur par défaut depuis la zone de liste **Store Event Payload** list dans la fenêtre QRadar Settings sur l'onglet **Admin**. Cependant, lorsque vous créez une nouvelle source de journal ou mettez à jour la configuration pour reconnaître automatiquement la source de journal, vous pouvez redéfinir la valeur par défaut en configurant cette case pour chaque source de journal. Pour plus d'informations sur les paramètres, voir *IBM Security QRadar Administration Guide*.
File Upload tab	Vous permet d'importer un fichier texte contenant un maximum de 500 adresses IP ou de noms d'hôte des sources de journal que souhaitez ajouter en vrac. Le fichier texte doit contenir une adresse IP ou un nom d'hôte par ligne. Des caractères supplémentaires après une adresse IP ou des noms d'hôte de plus de 255 caractères créent une erreur indiquant qu'une source de journal à partir de la liste d'hôtes ne peut pas être ajoutée.
Domain Query tab	Vous permet de rechercher un domaine et des sources de journal en vrac à partir d'un contrôleur de domaine. Pour rechercher un domaine vous devez ajouter le domaine, le nom d'utilisateur et le mot de passe avant d'interroger le domaine pour les hôtes à ajouter. Saisissez les valeurs pour les paramètres suivants : • **Domain Controller** : Entrez l'adresse IP du contrôleur de domaine. • **Full Domain Name** : Entrez un nom de domaine valide.
Manual tab	Vous permet d'ajouter manuellement une adresse IP ou un nom d'hôte à la liste d'hôtes.
Add	Le champ add s'affiche lorsque vous avez au moins une source de journal dans la liste d'hôtes. Par défaut, la case est cochée. La désélection des cases dans le champ add permet d'ignorer une source de journal. ***Remarque :*** *Vous n'êtes pas obligé de décocher les cases pour les sources de journal qui existent déjà. Les doublons de noms d'hôtes ou les adresses IP sont ignorés.*

Etape 6 Cliquez sur **Save**.

Un récapitulatif des sources de journal ajoutées s'affiche.

Etape 7 Cliquez sur **Continue**.

Les sources de journal sont ajoutées à QRadar.

Edition de plusieurs sources de journal

Les sources de journal qui partagent un protocole commun peuvent être modifiées en tant que groupe puisqu'elles ont une même configuration.

Remarque : Vous pouvez utiliser la modification en vrac pour mettre à jour les noms d'hôte ou les adresses IP, mais vous ne pouvez pas supprimer les sources de journal. Pour plus d'informations, voir **Suppression d'une source de journal**.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Sélectionnez plusieurs sources de journal pour les modifier dans la liste.

Vous devez sélectionner une ou plusieurs sources de journal dans la liste des sources de journal actives pour la zone de liste **Bulk Edit** disponible.

Remarque : Pour modifier le nom, la description, l'identificateur de la source de journal ou le groupe, cliquez deux fois sur la sources de journal en vrac.

Etape 5 Pour utiliser la zone de liste **Bulk Actions,** sélectionnez **Bulk Edit**.

Etape 6 Entrez les valeurs des paramètres à modifier.

Pour plus d'informations, voir **Tableau 1-2**.

Etape 7 Cliquez sur **Save**.

Etape 8 Cliquez sur **Continue**.

La mise à jour de vos sources de journal est temrinée.

Configuration de protocoles de source de journal

Lorsque vous sélectionnez le type de source de journal dans la zone de liste Log Source Type**,** les options du protocole pour la source de journal sélectionnée s'affichent dans la zone de liste Protocol Configuration.

Cette section fournit des informations sur la configuration des protocoles suivants :

- **Syslog**
- **JDBC**
- **JDBC - SiteProtector**
- **Sophos Enterprise Console - JDBC**
- **Juniper Networks NSM**
- **OPSEC/LEA**
- **SDEE**
- **SNMPv1**
- **SNMPv2**
- **SNMPv3**
- **Sourcefire Defense Center Estreamer**

- **La source du protocole de fichier de journal autorise QRadar à récupérer les fichiers de journal archivés contenant les événements d'un hôte distant.**
- **Microsoft Security Event Log**
- **Microsoft Security Event Log Custom**
- **Microsoft Exchange**
- **Microsoft DHCP**
- **Microsoft IIS**
- **EMC VMWare**
- **SMB Tail**
- **Oracle Database Listener**
- **Cisco Network Security Event Logging**
- **Protocole PCAP Syslog Combination**
- **Protocole transféré**
- **Protocol TLS Syslog**
- **Protocole Juniper Security Binary Log Collector**
- **UDP Multiline Syslog Protocol**
- **TCP Multiline Syslog Protocol**
- **Protocole IBM Tivoli Endpoint Manager SOAP**

Syslog Pour configurer le protocole syslog, vous devez définir l'adresse IP ou le nom d'hôte du périphérique dans la zone Log Source Identifier.

L'adresse de l'identificateur doit être le périphérique de la source fournissant les événements à QRadar. Par exemple, si votre réseau contient plusieurs unités et une console de gestion, vous devez spécifier l'adresse IP de l'unité individuelle dans le champ Log Source Identifier. Cela permet aux événements transférés vers QRadar de contenir l'adresse IP ou le nom d'hôte de la source d'événement, au lieu de la console de gestion.

Tableau 1-3 Paramètres de protocole Syslog

Paramètre	Description
Log Source Identifier	Saisissez l'adresse IP ou le nom d'hôte de la source de journal en tant qu'identifiant pour des événements à partir de votre source d'événement syslog.

JDBC Pour configurer le protocole JDBC, définissez les valeurs des paramètres suivants :

Tableau 1-4 Paramètres de protocole JDBC

Paramètre	Description
Log Source Identifier	Saisissez les identifiants de la source de journal sous le format suivant : **<database>@<hostname>** or **<table name>|<database>@<hostname>** Où : **<table name>** correspond au nom du tableau ou vue de la base de données contenant les enregistrements d'événement. Ce paramètre est facultatif. Si vous incluez le nom du tableau, vous devez inclure une barre verticale (|) et le nom du tableau doit correspondre au paramètre Table Name. **<database>** correspond au nom de la base de données tel que défini dans le paramètre Database Name. Le nom de la base de données est un paramètre obligatoire. **<hostname>** est le nom d'hôte ou l'adresse IP de cette source de journal, tel que défini dans le paramètre IP or Hostname. Le nom d'hôte est un paramètre obligatoire. L'identificateur de source de journal doit être unique pour le type de source de journal.
Database Type	Dans la zone de liste, sélectionnez le type de base de données à utiliser pour la source d'événement. Les options incluent MSDE, Postgres, MySQL, Sybase et Oracle. L'option par défaut est MSDE.
Database Name	Entrez le nom de la base de données à laquelle vous souhaitez vous connecter. Le nom peut contenir jusqu'à 255 caractères alphanumériques. Le nom peut inclure les caractères spéciaux suivants : le symbole du dollar ($), le signe dièse (#), le trait de soulignement (_), le tiret (-) et le point (.).
IP or Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur de base de données.

Tableau 1-4 Paramètres de protocole JDBC (suite)

Paramètre	Description
Port	Entrez le numéro de port utilisé par le serveur de base de données. La valeur par défaut affichée dépend du Database Type sélectionné. L'intervalle valide est de 0 à 65536. Les valeurs par défaut incluent : • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Oracle - 1521 • Sybase - 1521 Le port de la configuration JDBC doit correspondre au port d'écoute de la base de données. La base de données doit posséder des connexions TCP entrantes activées pour communiquer avec QRadar. ***Remarque :*** *Si vous définissez une instance de base de données lors de l'utilisation de MSDE en tant que type de base de données, vous devez ne pas renseigner le paramètre Port dans votre configuration.*
Username	Entrez le nom d'utilisateur de la base de données. Le nom d'utilisateur peut contenir jusqu'à 255 caractères alphanumériques. Le nom d'utilisateur peut inclure des traits de soulignement (_).
Password	Entrez le mot de passe de la base de données. Le mot de passe peut contenir jusqu'à 225 caractères.
Confirm Password	Confirmez le mot de passe pour accéder à la base de données.
Authentication Domain	Si vous sélectionnez MSDE comme type de base de données et que la base de données est configurée pour Windows, vous devez définir un domaine d'authentification Windows. Sinon, laissez ce champ vide. Le domaine d'authentification doit contenir des caractères alphanumériques. Le domaine doit inclure les caractères spéciaux suivants : le trait de soulignement (_), le tiret (-)et la période (.).
Database Instance	Si vous définissez le type de données MSDE et que vous disposez de plusieurs instances de serveur sur un serveur, définissez l'instance à laquelle vous souhaitez vous connecter. ***Remarque :*** *Si vous utilisez un port non standard dans votre configuration de base de données ou que vous avez bloqué l'accès au port 1434 pour résoudre la base de données SQL, vous devez ne pas renseigner le paramètre Database Instance dans votre configuration.*

Tableau 1-4 Paramètres de protocole JDBC (suite)

Paramètre	Description
Table Name	Entrez le nom du tableau ou de la vue qui inclut les enregistrements d'événement. Le nom du tableau peut contenir jusqu'à 255 caractères alphanumériques. Le nom de la table peut inclure les caractères spéciaux suivants : dollar ($), dièse (#), trait de soulignement (_), tiret (-) et point (.).
Select List	Entrez la liste des champs à inclure dans les événements. Vous pouvez utiliser une liste séparée par des virgules ou saisir * pour tous les champs du tableau ou de la vue. Vous pouvez utiliser une liste séparée par des virgules pour définir les champs spécifiques des tableaux ou des vues. La liste doit contenir le champ défini dans le paramètre Compare Field. La liste séparée par des virgules peut contenir jusqu'à 255 caractères alphanumériques. La liste peut inclure les caractères spéciaux suivants : le symbole du dollar ($), le signe dièse (#), le trait de soulignement (_), le tiret (-) et le point (.).
Compare Field	Entrez un champ valeur numérique ou horodatage à utiliser pour identifier les nouveaux événements ajoutés entre les analyses et le tableau. Le champ de comparaison du tableau peut contenir jusqu'à 255 caractères alphanumériques. La liste peut inclure les caractères spéciaux suivants : le symbole du dollar ($), le signe dièse (#), le trait de soulignement (_), le tiret (-) et le point (.).
Start Date and Time	Facultatif. Configurez la date et l'heure de début pour l'interrogation de la base de données. Le paramètre Start Date and Time doit être au format aaaa-mm-jj HH:mm avec la spécification HH à l'aide d'une horloge au format 24 heures. Si la date ou l'heure de début est claire, l'interrogation commence immédiatement et se répète sur l'intervalle d'interrogation spécifié.
Use Prepared Statements	Sélectionnez cette case pour utiliser des instructions préparées. Les instructions préparées permettent à la source du protocole JDBC de configurer l'instruction SQL puis d'exécuter l'instruction SQL plusieurs fois avec des paramètres différents. Pour des raisons de sécurité et de performance, nous vous recommandons d'utiliser les instructions préparées. Désélectionnez cette case pour utiliser une méthode alternative d'interrogation qui n'utilise pas des instructions précompilées.
Polling Interval	Saisissez l'intervalle d'interrogation qui correspond au nombre d'heures entre les interrogations et la table d'événements. L'intervalle d'interrogation par défaut est de 10 secondes. Vous pouvez définir un plus long intervalle d'interrogation en ajoutant H pour les heures ou M pour les minutes à la valeur numérique. L'intervalle d'interrogation maximum est 1 semaine sous tous les formats d'heure. Les valeurs numériques sans un sondage identificateur H ou M en secondes.

Tableau 1-4 Paramètres de protocole JDBC (suite)

Paramètre	Description
EPS Throttle	Entrez le nombre d'événements par seconde (EPS) que vous souhaitez pas que ce protocole dépasse. La valeur par défaut est de 20000 EPS.
Use Named Pipe Communication	Si vous choisissez MSDE comme type de base de données, sélectionnez la case pour utiliser une méthode alternative à une connexion de port TCP/IP. Lorsque vous utilisez une connexion à un canal de communication nommé, le nom d'utilisateur et le mot de passe doivent être ceux de l'authentification Windows appropriée et non ceux de la base de données. De plus, vous devez utiliser le canal de communication nommé par défaut.
Database Cluster Name	Si vous sélectionnez la case **Use Named Pipe Communication**, le paramètre Database Cluster Name s'affiche. Si vous exécutez votre serveur SQL dans un environnement cluster, définissez le nom du cluster pour s'assurer que le canal de communication nommé fonctionne correctement.
Use NTLMv2	Si vous sélectionnez MSDE comme Type de base de données, la case à cocher **Use NTLMv2** s'affiche. Sélectionnez la case **Use NTLMv2** pour forcer les connexions MSDE à utiliser le protocole NTLMv2 lorsque vous communiquez avec des serveurs SQL qui nécessitent l'authentification NTLMv2. La valeur par défaut de la case à cocher est sélectionnée. Si la case **Use NTLMv2** est sélectionnée, elle n'a aucun effet sur les connexions MSDE aux serveurs SQL qui ne requièrent pas une authentification NTLMv2.

Installation de MySQL Connector/J Driver

IBM Security QRadar Les éditions de maintenance 3 et supérieures ne sont pas installées avec un pilote MySQL pour JDBC. Si vous utilisez un DSM ou un protocole qui nécessite un pilote MySQL JDBC, vous devez télécharger et installer l'élément MySQL Connector/J indépendant de la plateforme à partir de *http://dev.mysql.com/downloads/connector/j/.*

Pour installer le pilote MySQL JDBC :

Etape 1 Téléchargez le pilote MySQL JDBC à partir du site Web suivant :

http://dev.mysql.com/downloads/connector/j/

Etape 2 Copiez les fichiers.zip ou tar.gz MySQL Connector/J vers votre QRadar ou votre Collecteur d'événements.

Etape 3 Entrez ceci pour extraire le fichier.zip ou le fichier tar.gz de votre dispositif :

- Pour les fichiers.zip : **`gzip -d mysql-connector-java-<version>.zip`**
- Pour les fichiers tar.gz : **`tar -zxvf mysql-connector-java-<version>.tar.gz`**

Le fichier.zip ou tar.gz extrait contient le fichier mysql-connector-java-<version>.jar. Les fichiers extraits se trouvent dans un dossier mysql-connector-java-<version>

Etape 4 Accédez au dossier mysql-connector-java-<version>

Etape 5 Entrez ceci pour copier le fichier JAR MySQL Connector/J vers le répertoire adéquat :

```
cp mysql-connector-java-<version>-bin.jar /opt/qradar/jars
```

Etape 6 Entrez la commande suivante pour redémarrer Tomcat :

```
redémarrage du service tomcat
```

Etape 7 Entrez la commande suivante pour redémarrer Event Collection System (ECS) :

```
redémarrage du service ecs
```

ATTENTION : *Le redémarrage du service Event Collection System (ECS) suspend toute la collecte d'événements pour QRadar jusqu'au redémarrage du service.*

Après le redémarrage du service, l'installation du pilote MySQL est terminée. Pour plus d'informations sur l'installation ou l'utilisation de MySQL Connector/J, voir http://dev.mysql.com/downloads/connector/j/.

JDBC - SiteProtector

Le protocole JDBC - SiteProtector combine les informations depuis les tableaux SensorData1 et SensorDataAVP1 dans la création du contenu de la source de journal.

Les tableaux SensorData1 et SensorDataAVP1 se trouvent dans la base de données d'IBM Proventia® Management SiteProtector®.

Remarque : Le nombre maximal de lignes que le protocole JDBC - SiteProtector peut sonder en une analyse unique est de 30000 lignes.

Pour configurer le protocole JDBC - SiteProtector, définissez les valeurs des paramètres suivants :

Tableau 1-5 Paramètres de protocole JDBC

Paramètre	Description
Log Source Identifier	Saisissez les identifiants de la source de journal sous le format suivant : **<database>@<hostname>** Où : **<database>** correspond au nom de la base de données tel que défini dans le paramètre Database Name. Le nom de la base de données est un paramètre obligatoire. **<hostname>** est le nom d'hôte ou l'adresse IP de la source de journal tel que défini dans le paramètre de l'adresse IP ou de l'hôte. Le nom d'hôte est un paramètre obligatoire. L'identificateur de source de journal doit être unique pour le type de source de journal.
Database Type	Dans la zone de liste, sélectionnez **MSDE** en tant type de base de données à utiliser pour la source d'événement.
Database Name	Entrez le nom de la base de données à laquelle vous souhaitez vous connecter. Le nom de la base de données par défaut est **RealSecureDB**. Le nom du tableau peut contenir jusqu'à 255 caractères alphanumériques. Le nom de la table peut inclure les caractères spéciaux suivants : dollar ($), dièse (#), trait de soulignement (_), tiret (-) et point (.).
IP or Hostname	Entrez l'adresse IP ou le nom d'hôte du serveur de base de données.

Tableau 1-5 Paramètres de protocole JDBC (suite)

Paramètre	Description
Port	Entrez le numéro de port utilisé par le serveur de base de données. La valeur par défaut qui est affichée dépend du Database Type sélectionné. L'intervalle valide est compris entre 0 à 65536. La valeur par défaut du MSDE est le port 1433. Le port de la configuration JDBC doit correspondre au port d'écoute de la base de données. La base de données doit posséder des connexions TCP entrantes activées pour communiquer avec QRadar. Le port par défaut pour toutes les options inclut : • **MSDE** - 1433 • **Postgres** - 5432 • **MySQL** - 3306 • **Oracle** - 1521 • **Sybase** - 1521 ***Remarque :*** *Si vous définissez une instance de base de données lors de l'utilisation de MSDE en tant que type de base de données, vous devez ne pas renseigner le paramètre Port dans votre configuration.*
Username	Entrez le nom d'utilisateur de la base de données. Le nom d'utilisateur peut contenir jusqu'à 255 caractères alphanumériques. Le nom d'utilisateur peut également inclure des traits de soulignement (_).
Password	Entrez le mot de passe de la base de données. Le mot de passe peut contenir jusqu'à 225 caractères.
Confirm Password	Confirmez le mot de passe pour accéder à la base de données.
Authentication Domain	Si vous sélectionnez MSDE comme type de base de données et que la base de données est configurée pour Windows, vous devez définir un domaine d'authentification Windows. Sinon, laissez ce champ vide. Le domaine d'authentification doit contenir des caractères alphanumériques. Le domaine doit inclure les caractères spéciaux suivants : le trait de soulignement (_), le tiret (-)et la période (.).
Database Instance	Si vous définissez le type de données MSDE et que vous disposez de plusieurs instances de serveur sur un serveur, définissez l'instance à laquelle vous souhaitez vous connecter. ***Remarque :*** *Si vous utilisez un port non standard dans votre configuration de base de données ou que vous avez bloqué l'accès au port 1434 pour résoudre la base de données SQL, vous devez ne pas renseigner le paramètre Database Instance dans votre configuration.*

Tableau 1-5 Paramètres de protocole JDBC (suite)

Paramètre	Description
Table Name	Entrez le nom du tableau ou de la vue qui inclut les enregistrements d'événement. Le nom de la table par défaut est **`SensorData1.`** Le nom du tableau peut contenir jusqu'à 255 caractères alphanumériques. Le nom de la table peut inclure les caractères spéciaux suivants : dollar ($), dièse (#), trait de soulignement (_), tiret (-) et point (.).
Select List	Entrez **`*`** pour inclure tous les champs à partir de la table ou de la vue. Vous pouvez utiliser une liste séparée par des virgules pour définir les champs spécifiques à partir des tableaux ou des vues, si nécessaire dans votre configuration. La liste doit contenir le champ défini dans le paramètre Compare Field. La liste séparée par des virgules peut contenir jusqu'à 255 caractères alphanumériques. La liste peut inclure les caractères spéciaux suivants : le symbole du dollar ($), le signe dièse (#), le trait de soulignement (_), le tiret (-) et le point (.).
Compare Field	Entrez **`SensorDataRowID`** pour identifier les nouveaux événements ajoutés entre les requêtes et la table. Le champ de comparaison du tableau peut contenir jusqu'à 255 caractères alphanumériques. La liste peut inclure les caractères spéciaux : le symbole du dollar ($), le signe dièse (#), le trait de soulignement (_), le tiret (-) et la période(.).
Start Date and Time	Facultatif. Configurez la date et l'heure de début pour l'interrogation de la base de données. Le paramètre Start Date and Time doit être au format aaaa-mm-jj HH:mm avec la spécification HH à l'aide d'une horloge au format 24 heures. Si la date ou l'heure de début est claire, l'interrogation commence immédiatement et se répète sur l'intervalle d'interrogation spécifié.
Use Prepared Statements	Cochez cette case pour utiliser les instructions préparées qui permettent à la source du protocole JDBC de configurer l'instruction SQL à temps, puis exécuter l'instruction SQL plusieurs fois avec des paramètres. Pour la sécurité et de performance, nous vous recommandons d'utiliser les instructions préparées. Désélectionnez cette case pour utiliser une méthode alternative d'interrogation qui n'utilise pas des instructions précompilées.
Include Audit Events	Cochez cette case pour collecter les événements d'audit à partir d'IBM SiteProtector®. Par défaut, cette case est désélectionnée.

Tableau 1-5 Paramètres de protocole JDBC (suite)

Paramètre	Description
Polling Interval	Saisissez l'intervalle d'interrogation qui correspond au nombre d'heures entre les interrogations et la table d'événements. L'intervalle d'interrogation par défaut est de 10 secondes. Vous pouvez définir un plus long intervalle d'interrogation en ajoutant H pour les heures ou M pour les minutes à la valeur numérique. L'intervalle d'interrogation maximum est 1 semaine sous tous les formats d'heure. Les valeurs numériques sans un sondage identificateur H ou M en secondes.
Use Named Pipe Communication	Si vous choisissez MSDE comme Type de base de données, sélectionnez cette case pour utiliser une méthode alternative à une connexion de port TCP/IP. Lorsque vous utilisez une connexion à un canal de communication nommé, le nom d'utilisateur et le mot de passe doivent être ceux de l'authentification Windows appropriée et non ceux de la base de données. De plus, vous devez utiliser le canal de communication nommé par défaut.
Database Cluster Name	Si vous sélectionnez la case Use Named Pipe Communication, le paramètre Database Cluster Name s'affiche. Si vous exécutez votre serveur SQL dans un environnement cluster, définissez le nom du cluster pour s'assurer que le canal de communication nommé fonctionne correctement.

Sophos Enterprise Console - JDBC

La Sophos Enterprise Console - Le protocole de connectivité JDBC combine des informations de contenu à partir des journaux de contrôle d'application, de périphériques, de données, de protection et de pare-feu dans le tableau vEventsCommonData pour fournir les événements à QRadar.

Remarque : Si votre Sophos Enterprise Console ne dispose pas de l'interface de rapports Sophos, vous pouvez collecter les événements Anti-Virus via le protocole de connectivité JDBC. Pour plus d'informations sur la configuration de Sophos Enterprise Console via le protocole JDBC, consultez le Guide de configuration *DSM*.

Pour utiliser la Sophos Enterprise Console - le protocole de connectivité JDBC, vous devez vous assurer que la Sophos Reporting Interface est installée avec votre Sophos Enterprise Console.

Si la Sophos Reporting Interface est installée, vous pouvez configurer les valeurs des paramètres suivants :

Tableau 1-6 Paramètres de protocole Sophos Enterprise Console JDBC

Paramètre	Description
Log Source Identifier	Saisissez les identifiants de la source de journal sous le format suivant : **<Sophos Database>@<Sophos Database Server IP ou Host Name>** Où : **<Sophos Database>** correspond au nom de la base de données tel qu'entré dans le paramètre Database Name. **<Sophos Database Server IP or Host Name>** est le nom d'hôte ou l'adresse IP de cette source de journal, tel qu'entré dans le paramètre de l'adresse IP ou de l'hôte. ***Remarque :*** *En définissant un nom pour votre identifiant de source de journal, vous devez voir les valeur de l'adresse IP ou du nom d'hôte de Sophos Database et Database Server IP address à partir de Management Enterprise Console.*
Database Type	Dans la zone de liste, cochez **MSDE**.
Database Name	Entre le nom exact de la base de données Sophos.
IP or Hostname	Entrez l'adresse IP ou le nom d'hôte de Sophos SQL Server.
Port	Entrez le numéro de port utilisé par le serveur de base de données. Le port par défaut pour MSDE dans Sophos Enterprise Console est 1168. Le port de la configuration JDBC doit correspondre au port d'écoute de la base de données Sophos. La base de données Sophos doit avoir des connections TCP entrantes activées pour communiquer avec QRadar. ***Remarque :*** *Si vous définissez une instance de base de données lors de l'utilisation de MSDE en tant que type de base de données, vous devez ne pas renseigner le paramètre Port dans votre configuration.*
Username	Entrez le nom d'utilisateur requis pour accéder à la base de données.
Password	Entrez le mot de passe requis pour accéder à la base de données. Le mot de passe peut contenir jusqu'à 225 caractères.
Confirm Password	Confirmez le mot de passe requis pour accéder à la base de données. Le mot de passe de confirmation doit être identique à celui du mot de passe entré dans le paramètre de mot de passe.
Authentication Domain	Si vous sélectionnez MSDE comme type de base de données et que la base de données est configurée pour Windows, vous devez définir un domaine d'authentification Window. Sinon, laissez ce champ vide.

Tableau 1-6 Paramètres de protocole Sophos Enterprise Console JDBC (suite)

Paramètre	Description
Database Instance	Facultatif. Entrez l'instance de base de données, si vous avez des instances de serveur SQL sur votre serveur de base de données. ***Remarque :*** *Si vous utilisez un port non standard dans votre configuration de base de données ou que vous avez bloqué l'accès au port 1434 pour résoudre la base de données SQL, vous devez ne pas renseigner le paramètre Database Instance dans votre configuration.*
Table Name	Entrez **vEventsCommonData** comme nom du tableau ou de la vue qui inclut les enregistrements d'événement.
Select List	Entrez ***** pour tous les champs à partir de la table ou de la vue. Vous pouvez utiliser une liste séparée par des virgules pour définir les champs spécifiques à partir des tableaux ou des vues. La liste doit contenir le champ défini dans le paramètre Compare Field. La liste séparée par des virgules peut contenir jusqu'à 255 caractères alphanumériques. La liste peut inclure les caractères spéciaux suivants : le symbole du dollar ($), le signe dièse (#), le trait de soulignement (_), le tiret (-) et le point (.).
Compare Field	Entrez **InsertedAt** en tant que champ de comparaison. Le champ de comparaison est utilisé pour identifier les nouveaux événements ajoutés entre les requêtes et la table.
Start Date and Time	Facultatif. Entrez la date et l'heure de début pour l'interrogation de la base de données. Le paramètre Start Date and Time doit être au format aaaa-mm-jj HH:mm avec la spécification HH à l'aide d'une horloge au format 24 heures. Si la date ou l'heure de début est claire, l'interrogation commence immédiatement et se répète sur l'intervalle d'interrogation spécifié.
Polling Interval	Saisissez l'intervalle d'interrogation qui correspond au nombre d'heures entre les interrogations et la table d'événements. L'intervalle d'interrogation par défaut est de 10 secondes. Vous pouvez définir un plus long intervalle d'interrogation en ajoutant H pour les heures ou M pour les minutes à la valeur numérique. L'intervalle d'interrogation maximum est 1 semaine sous tous les formats d'heure. Les valeurs numériques entrées sans une requête H or M en secondes.
EPS Throttle	Entrez le nombre d'événements par seconde (EPS) que vous ne souhaitez pas que ce protocole dépasse. La valeur par défaut est de 20000 EPS.
Use Named Pipe Communication	Décochez la case Use Named Pipe Communications. Lorsque vous utilisez une connexion à un canal de communication nommé, le nom d'utilisateur et le mot de passe doivent être ceux de l'authentification Windows appropriée et non ceux de la base de données. De plus, vous devez utiliser le canal de communication nommé par défaut.

Tableau 1-6 Paramètres de protocole Sophos Enterprise Console JDBC (suite)

Paramètre	Description
Database Cluster Name	Si vous sélectionnez la case Use Named Pipe Communication, le paramètre Database Cluster Name s'affiche. Si vous exécutez votre serveur SQL dans un environnement cluster, définissez le nom du cluster pour s'assurer que le canal de communication nommé fonctionne correctement.
Use NTLMv2	Si vous sélectionnez MSDE comme Type de base de données, la case à cocher **Use NTLMv2** s'affiche. Sélectionnez la case **Use NTLMv2** pour forcer les connexions MSDE à utiliser le protocole NTLMv2 lorsque vous communiquez avec des serveurs SQL qui nécessitent l'authentification NTLMv2. La valeur par défaut de la case à cocher est sélectionnée. Si la case **Use NTLMv2** est sélectionnée, elle n'a aucun effet sur les connexions MSDE aux serveurs SQL qui ne requièrent pas une authentification NTLMv2.

Juniper Networks NSM

Pour configurer le protocole Juniper Networks NSM, définissez les valeurs des paramètres suivants :

Tableau 1-7 Paramètres de protocole Juniper NSM

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour la source d'événement. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
IP	Entrez l'adresse IP ou le nom d'hôte du serveur Juniper Networks NSM.
Inbound Port	Entrez le port par lequel Juniper Networks NSM envoie les communications. L'intervalle valide est entre 0 et 65536. La valeur par défaut est de 514.
Redirection Listen Port	Spécifie le port auquel le trafic est transmis. L'intervalle valide est entre 0 et 65 536. La valeur par défaut est de 516.
Use NSM Address for Log Source	Cochez cette case si vous souhaitez utiliser l'adresse IP du serveur Juniper NSM au lieu de l'adresse IP de la source de journal gérée d'une source de journal. Par défaut, la case est cochée.

OPSEC/LEA

Pour configurer le protocole OPSEC/LEA, définissez les valeurs des paramètres suivants :

Tableau 1-8 Paramètres de protocole OPSEC/LEA

Paramètre	Description
Log Source Identifier	Saisissez l'adresse IP de la source de journal. Cette valeur doit correspondre à la valeur configurée dans le paramètre Server IP. L'identificateur de source de journal doit être unique pour le type de source de journal.
Server IP	Entrez l'adresse IP du serveur.
Server Port	Entrez le port utilisé pour la communication OPSEC. L'intervalle valide est entre 0 et 65 536 et La valeur par défaut est de 18184.
Use Server IP for Log Source	Cochez cette case si vous souhaitez utiliser l'adresse IP du serveur LEA à la place de l'adresse IP de l'unité gérée d'une source de journal. Par défaut, la case est cochée.
Statistics Report Interval	Entrez l'intervalle, en secondes, pendant lequel le nombre d'événements syslog sont enregistrés dans le fichier qradar.log. L'intervalle valide est entre 4 et 2.147.483.648 et La valeur par défaut est de 600.

Tableau 1-8 Paramètres de protocole OPSEC/LEA (suite)

Paramètre	Description
Authentication Type	Dans la zone de liste, sélectionnez l'authentification que vous souhaitez utiliser pour cette configuration LEA. Les options sont **sslca** (par défaut), **sslca_clear** ou **clear**. Cette valeur doit correspondre à la méthode d'authentification utilisée par le serveur. Les paramètres suivants apparaissent si vous sélectionnez sslca ou sslca_clear comme type d'authentification. • **OPSEC Application Object SIC Attribute (Nom de SIC)** : Entrez le nom de SIC (Secure Internal Communications) de l'OPSEC Application Object. Le nom du SIC est le nom distinctif (DN) de l'application, par exemple : **`CN=LEA, o=fwconsole..7psasx.`** Le nom peut contenir jusqu'à 225 caractères et est sensible à la casse. • **Log Source SIC Attribute (Nom de SIC de l'entité)** - Entrez le nom de SIC du serveur, par exemple : **`cn=cp_mgmt,o=fwconsole..7psasx.`** Le nom peut contenir jusqu'à 225 caractères et est sensible à la casse. • **Specify Certificate** - Sélectionnez cette case si vous souhaitez définir un certificat pour cette configuration LEA. QRadar tente de récupérer le certificat à l'aide de ces paramètre lorsque le certificat est requis. Si vous sélectionnez la case **Specify Certificate**, le paramètre Certificate Filename s'affiche : • **Certificate Filename** : Cette option ne s'affiche que si vous avez sélectionné Specify Certificate. Entrez le chemin de répertoire du certificat que vous souhaitez utiliser pour cette configuration. Si vous désélectionnez la case **Specify Certificate**, les paramètres suivants apparaissent : • **Certificate Authority IP** : Entrez l'adresse IP du serveur SmartCenter à partir de laquellevous souhaitez extraire votre certificat. • **Pull Certificate Password** : Entrez le mot de passe que vous souhaitez utiliser lorsque vous demandez un certificat. Le mot de passe peut contenir jusqu'à 225 caractères. • **OPSEC Application** : Entrez le nom que vous souhaitez utiliser lorsque vous demandez un certificat. La valeur peut contenir jusqu'à 225 caractères.

SDEE Pour configurer le protocole SDEE, définissez les valeurs des paramètres suivants :

Tableau 1-9 Paramètres de protocole SDEE

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement SDEE. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
URL	Entrez l'adresse URL requise pour accéder à la source du journal source, par exemple, https://www.mysdeeserver.com/cgi-bin/sdee-server. Vous devez utiliser une URL http ou https. Les options incluent : • Si vous utilisez SDEE/CIDEE (pour Cisco IDS v5.x et plus), l'adresse URL doit contenir /cgi-bin/sdee-server à la fin. Par exemple, **`https://www.my-sdee-server/cgi-bin/sdee-server`** • Si vous utilisez RDEP (pour Cisco IDS v4.0), l'adresse URL doit contenir /cgi-bin/event-server à la fin. Par exemple, **`https://www.my-rdep-server.com/cgi-bin/event-server`**
Username	Saisissez le nom d'utilisateur. Ce nom d'utilisateur doit correspondre au nom d'utilisateur URL SDEE utilisé pour accéder à l'URL SDEE. Le nom d'utilisateur peut contenir jusqu'à 255 caractères.
Password	Saisissez le mot de passe de l'utilisateur. Ce mot de passe doit correspondre au mot de passe de l'URL SDEE utilisé pour accéder à l'URL SDEE. Le mot de passe peut contenir jusqu'à 225 caractères.
Events / Query	Entrez le nombre maximum d'événements à extraire par analyse. La plage valide est comprise entre 0 et 501. La valeur par défaut est de définie sur 100.
Force Subscription	Cochez cette case si vous souhaitez imposer un nouvel abonnement SDEE. Par défaut, la case est cochée. La case impose au serveur d'abandonner la connexion la moins active et d'accepter une nouvelle connexion d'abonnement SDEE pour cette source de journal. Si vous décochez la case, l'abonnement poursuit avec tout abonnement SDEE existant.
Severity Filter Low	Cochez cette case si vous souhaitez configurer un niveau de sécurité bas. Les sources de journal qui prennent en charge SDEE renvoient uniquement les événements qui correspondent à ce niveau de gravité. Par défaut, la case est cochée.

Tableau 1-9 Paramètres de protocole SDEE (suite)

Paramètre	Description
Severity Filter Medium	Cochez cette case si vous souhaitez configurer un niveau de sécurité moyen. Les sources de journal qui prennent en charge SDEE ne retournent que les événements qui correspondent à ce niveau de sécurité. Par défaut, la case est cochée.
Severity Filter High	Cochez cette case si vous souhaitez configurer un niveau de sécurité haut. Les sources de journal qui prennent en charge SDEE ne retournent que les événements qui correspondent à ce niveau de sécurité. Par défaut, la case est cochée.

SNMPv1 Pour configurer le protocole SNMPv1, vous devez saisir l'adresse IP de la source de journal dans le paramètre Log Source Identifier. L'identificateur de la source de journal doit être unique pour le type de source de journal.

SNMPv2 Pour configurer le protocole SNMPv2, définissez les valeurs des paramètres suivants :

Tableau 1-10 Paramètres de protocole SNMPv2

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour la source d'événement SNMPv2. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Community	Saisissez le nom de communauté SNMP requis pour accéder au système contenant les événements SNMP. Public est choisi par défaut.
Include OIDs in Event Payload	Cette option permet à la charge utile d'événement SNMP d'être construite à l'aide de paires nom-valeur au lieu du format de charge utile d'événement standard. Il est obligatoire d'inclure des OID dans la charge utile d'événement pour traiter les événements SNMPv2 ou SNMPv3 à partir de certains DSM. Pour plus d'informations, voir le Guide de configuration *DSM.*

SNMPv3 Pour configurer le protocole SNMPv3, définissez les valeurs des paramètres suivants :

Tableau 1-11 Paramètres de protocole SNMPv3

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour la source d'événement SNMPv2. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.

Tableau 1-11 Paramètres de protocole SNMPv3 (suite)

Paramètre	Description
Authentication Protocol	Dans la zone de liste, sélectionnez l'algorithme que vous souhaitez utiliser pour authentifier les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. La valeur par défaut est de MD5.
Authentication Password	Entrez le mot de passe que vous souhaitez utiliser pour authentifier SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. Le mot de passe peut contenir jusqu'à 64 caractères. ***Remarque :*** *Votre mot de passe d'authentification doit inclure 8 caractères au minimum.*
Decryption Protocol	Dans la zone de liste, sélectionnez le protocole que vous souhaitez utiliser pour déchiffrer les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. AES256 est choisi par défaut.
Decryption Password	Entrez le mot de passe utilisé pour déchiffrer les alertes SNMP. Ce paramètre est obligatoire si vous utilisez SNMPv3. Le mot de passe peut contenir jusqu'à 64 caractères.
User	Entrez l'accès utilisateur pour ce protocole. AdminUser est choisi par défaut. Le nom d'utilisateur peut contenir jusqu'à 255 caractères.

Sourcefire Defense Center Estreamer

Le protocole Sourcefire Defense Center Estreamer permet à QRadar de recevoir les flux de données d'événements en continu depuis un service Sourcefire Defense Center Estreamer (Event Streamer).

Les fichiers d'événements sont compactés vers QRadar pour le traitement précédant la configuration Sourcefire Defense Center DSM. Pour plus d'informations sur votre Sourcefire Defense Center DSM, consultez le Guide de configuration *IBM Security QRadar DSM.*

Tableau 1-12 Paramètres de protocole Sourcefire Defense Center Estreamer

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement Sourcefire Defense Center. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Server Address	Entrez l'adresse IP ou le nom d'hôte du périphérique Sourcefire Defense Center.
Server Port	Entrez le numéro de port qu'utilise QRadar pour recevoir les événements Sourcefire Defense Center Estreamer. 8302 est coché par défaut.

Tableau 1-12 Paramètres de protocole Sourcefire Defense Center Estreamer (suite)

Paramètre	Description
Keystore Filename	Entrez le chemin de répertoire et le nom de fichier pour la clé privée du fichier de clés et le certificat associé. Par défaut, le script important crée le fichier de clés dans le répertoire suivant : **`/opt/qradar/conf/estreamer.keystore`**
Truststore Filename	Entrez le chemin de répertoire et le nom de fichier pour les fichiers de clés certifiées. Le fichier de clés certifiées contient les certificats sécurisés par le client. Par défaut, le script important crée le fichier de clés certifiées dans le répertoire suivant : **`/opt/qradar/conf/estreamer.truststore`**

Protocole de fichier de journal

La source du protocole de fichier de journal autorise QRadar à récupérer les fichiers de journal archivés contenant les événements d'un hôte distant.

Les fichiers du journal sont transférés, un par un vers QRadar pour leur traitement. Le protocole de fichier journal peut gérer le texte brut, les fichiers compressés ou les archives. Les archives doivent contenir des fichiers de textes bruts pouvant être traités ligne après ligne. Lorsqu'une source du protocole télécharge un fichier pour traitement, QRadar traite les informations reçues dans le fichier afin de générer des événements. Lorsque des informations supplémentaires sont inscrites dans le fichier à la fin du téléchargement, celles-ci ne sont pas traitées par QRadar.

Remarque : Le protocole Log File est conçu pour les fichiers qui génèrent quotidiennement des journaux d'événements. Il n'est pas recommandé d'utiliser le protocole Log File pour les unités qui ajoutent des informations supplémentaires à leurs fichiers d'événements.

Pour configurer le protocole Log File, définissez les valeurs des paramètres suivants :

Tableau 1-13 Paramètres de protocole Log File

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour la source d'événement. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique. Par exemple, si votre réseau contient plusieurs périphériques comme une console de gestion ou un référentiel de fichiers, vous devez spécifier l'adresse IP ou le nom d'hôte du périphérique qui a créé l'événement. Ceci permet d'identifier les événements au niveau du périphérique dans votre réseau au lieu d'identifier l'événement pour la console de gestion ou le référentiel de fichiers.
Service Type	Dans la zone de liste, sélectionnez le protocole que vous souhaitez utiliser lors de la récupération des fichiers journaux à partir d'un serveur distant. Par défaut SFTP est sélectionné. • **SFTP** : protocole SFTP • **FTP** : protocole FTP • **SCP** - Copie sécurisée ***Remarque :*** *Le protocole sous-jacent utilisé pour récupérer les fichiers journaux pour le type de serviceSCP et SFTP nécessite que le serveur spécifié dans le champ* ***Remote IP or Hostname*** *a activé le sous-système SFTP.*
Remote IP or Hostname	Entrez l'adresse IP ou le nom d'hôte du périphérique qui stocke vos événements de fichiers journaux.
Remote Port	Entrez le port TCP sur l'hôte distant qui exécute le type de service sélectionné. L'intervalle valide est compris entre 1 et 65535. Les options incluent : • **FTP** : port TCP 21 • **SFTP** : port TCP 22 • **SCP** : port TCP 22 ***Remarque :*** *Si l'hôte de vos fichiers d'événements utilise un numéro de port non standard pour FTP, SFTP ou SCP, vous devez ajuster la valeur du port en conséquence.*
Remote User	Entrez le nom d'utilisateur permettant de se connecter à l'hôte contenant vos fichiers d'événements. Le nom d'utilisateur peut contenir jusqu'à 255 caractères.
Remote Password	Entrez le mot de passe permettant de se connecter à l'hôte.
Confirm Password	Confirmez le mot de passe permettant de se connecter à l'hôte.

Tableau 1-13 Paramètres de protocole Log File (suite)

Paramètre	Description
SSH Key File	Si vous sélectionnez SCP ou SFTP en tant que type de service, ce paramètre vous permet de définir un fichier de clés privées SSH. Lorsque vous fournissez un fichier de clés SSH, le champ **Remote Password** est ignoré.
Remote Directory	Entrez l'emplacement du répertoire sur l'hôte distant à partir duquel les fichiers sont récupérés, relatifs au compte utilisateur que vous utilisez pour vous connecter. ***Remarque :*** *Uniquement pour FTP. Si vos fichiers journaux se trouvent dans le répertoire d'accueil de l'utilisateur distant, vous pouvez ne pas renseigner le répertoire distant. Ceci permet de prendre en charge le système d'exploitation dans lequel une modification dans la commande répertoire de travail (CWD) est restreinte.*
Recursive	Cochez la case si vous souhaitez que le masque de fichiers recherche les sous-dossiers. Par défaut, la case est décochée. L'option Recursive est ignorée si vous configurez SCP comme type de service.
FTP File Pattern	Si vous sélectionnez SFTP ou FTP comme type de service, cette option vous permet de confirmer l'expression régulière (regex) requise pour filtrer la liste des fichiers spécifiés dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement. Par exemple, pour lister tous les fichiers commençant par le mot log, suivi d'un ou de plusieurs chiffres et se terminant par **`tar.gz`**, utilisez l'entrée suivante : **`log[0-9]+\.tar\.gz`**. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
FTP Transfer Mode	Cette option ne s'applique que si vous sélectionnez FTP comme type de service. Le paramètre FTP Transfer Mode vous permet de définir le mode de transfert lors de la récupération de fichiers sur FTP. Dans la zone de liste, sélectionnez le mode de transfert que vous souhaitez appliquer à cette source de journal : • **Binary** : Sélectionnez Binary pour les sources de journaux qui requièrent des fichiers de données binaires ou des fichiers archive zip, gzip, tar ou tar+gzip compressés. • **ASCII** : Sélectionnez ASCII pour les sources de journaux qui requièrent un transfert de fichier ASCII FTP. Vous devez sélectionner **NONE** pour le paramètre Processor et **LINEBYLINE** pour le paramètre Event Generator lorsque vous utilisez ASCII comme FTP Transfer Mode.

Tableau 1-13 Paramètres de protocole Log File (suite)

Paramètre	Description
SCP Remote File	Si vous sélectionnez SCP comme le type de service vous devez entrer le nom de fichier du fichier distant.
Start Time	Entrez le moment de la journée auquel vous souhaitez démarrer le traitement. Ce paramètre fonctionne avec la valeur Recurrence pour définir quand et à quelle fréquence le répertoire distant est analysé pour les fichiers. Entrez l'heure de début, sur la base d'une horloge au format 24 heures, sous leformat suivant : HH:MM.
Recurrence	Entrez la fréquence en commençant par l'heure de début à laquelle vous souhaitez analyser le répertoire distant. Entrez cette valeur en heures (H), minutes (M) ou jours (D). Par exemple, 2H si vous souhaitez que le répertoire distant soit analysé toutes les 2 heures. La valeur par défaut est de 1H.
Run On Save	Sélectionnez cette case si vous souhaitez que le protocole s'exécute immédiatement après avoir cliqué sur Save. Après avoir terminé le Run On Save, le protocole du fichier journal suit la configuration de l'heure de début et de la programmation récurrente. La sélection de Run On Save supprime la liste des fichiers précédemment traités pour le paramètre Ignore Previously Processed File.
EPS Throttle	Entrez le nombre d'événements par seconde (EPS) que vous souhaitez pas que ce protocole dépasse. L'intervalle valide est compris entre 100 et 5000.
Processor	Si les fichiers qui se trouvent sur l'hôte distant sont stockés sous un format d'archive zip, gzip, tar, ou tar+gzip, sélectionnez le processeur qui permet de détailler les archives et de traiter le contenu.
Ignore Previously Processed File(s)	Cochez cette case pour pister les fichiers qui ont déjà été traités si vous ne souhaitez pas qu'ils soient traités une seconde fois. Ceci s'applique uniquement aux types de service FTP et SFTP.
Change Local Directory?	Sélectionnez cette case pour définir le répertoire local sur votre QRadar que vous souhaitez utiliser pour le stockage des fichiers enregistrés durant le traitement. Nous vous recommandons de ne pas cocher cette case. Lorsque vous cochez cette case, le répertoire local s'affiche, ce qui vous permet de configurer le répertoire local à utiliser pour le stockage des fichiers.

Tableau 1-13 Paramètres de protocole Log File (suite)

Paramètre	Description
Event Generator	Event Generator applique le traitement supplémentaire aux fichiers d'événements à récupérer. Dans la zone de liste **Event Generator**, sélectionnez les options suivantes : • **LineByLine** - Chaque ligne du fichier est traité en tant qu'événement unique. Par exemple, si un fichier comprend 10 lignes de texte, 10 événements séparés sont créés. • **HPTandem** : Le fichier est traité comme un journal d'audit binaire HPTandem/NonStop. Chaque enregistrement dans le fichier journal (primaire ou secondaire) est converti en texte et traité comme événement unique. Les journaux d'audit HPTandem utilisent le format de nom de fichier suivant : `"[aA]\d{7}"`. • **WebSphere Application Server** : Traite les fichiers journaux contenant les événements WebSphere Application Server générés dans WebSphere Application Server DSM. Le répertoire distant doit définir le chemin d'accès dans DSM. • **W3C** - Traite les fichiers journaux provenant des sources à l'aide du format w3c. L'en-tête du fichier journal identifie la commande et les données se trouvant sur chaque ligne du fichier. • **Fair Warning** - Traitez les fichiers journaux à partir des périphériques Fair Warning en protégeant l'identité et les informations médicales du patient. Le répertoire distant doit définir le chemin d'accès du fichier contenant les fichiers d'événements générés par votre périphérique Fair Warning. • **DPI Subscriber Data** : le fichier est traité comme un journal statique produit par un routeur Juniper Networks MX. L'en-tête du fichier identifie la commande et les données se trouvant sur chaque ligne du fichier. Chaque ligne dans le fichier après le formatage de l'en-tête à un événement de paire nom=valeur délimité par tabulation à traiter par QRadar. • **SAP Audit Logs** : Traitez les fichiers des journaux d'audit SAP pour conserver un enregistrement d'événements liés à la sécurité dans les systèmes SAP. Chaque ligne est formatée pour être traitée par QRadar. • **Oracle BEA WebLogic** : Traite les fichiers journal de l'application Oracle BEA WebLogic. Chaque ligne est formatée pour être traitée par QRadar. • **Juniper SBR** - Traite les fichiers journaux d'événement à partir de Juniper Steel-belted RADIUS. Chaque ligne est formatée pour être traitée par QRadar.

Microsoft Security Event Log

Le protocole Microsoft Security Event Log fournit la collection du journal d'événement dépourvue d'agents distants Windows pour Windows via l'interface de programme d'application Microsoft Windows Management Instrumentation (WMI).

Systèmes d'exploitation pris en charge

QRadar prend en charge l'interface de programme d'application Microsoft Windows Management Instrumentation suivant (WMI) :

- Microsoft Windows 2000
- Microsoft WIndows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R2
- Microsoft Windows XP
- Microsoft WIndows Vista
- Microsoft Windows 7

Types d'événements pris en charge

Le protocole Microsoft Windows Security Event Log est capable de collecter les types de journaux suivants :

- Application
- Security
- System
- DNS Server
- File Replication
- Directory Service logs

Avant de commencer

Vous devez configurer votre pare-feu pour accepter les communications externes entrantes sur le port 135 et tous les ports dynamiques, requis pour DCOM. Pour plus d'informations sur la configuration de DCOM, voir la documentation de Microsoft Support.

Les limites suivantes de la source de journal s'appliquent lors du déploiement du protocole de Microsoft Security Event Log dans votre environnement :

- Une installation QRadar unique peut prendre en charge plus de 250 sources de journaux à l'aide de Microsoft Security Event Log Protocol.
- Un collecteur d'événement dédié peut prendre en charge plus de 500 sources de journal à l'aide de Microsoft Security Event Log Protocol.

Remarque : Le protocole Microsoft Security Event Log n'est pas recommandé pour les serveurs distants, accessibles sur des liens réseau présentant des délais d'aller-retour très élevés, tel que le satellite ou les réseaux WAN lents. Le délai d'aller-retour peut être confirmé en examinant le temps de demande et de réponse

entre les serveurs à l'aide de la commande PING. Les délais de réseau créés par des connexions lentes diminuent le débit ESP disponible vers ces serveurs distants. En outre, la collection d'événement des serveurs occupés ou contrôleurs de domaine dépend de faibles délais d'aller-retour afin de maintenir les événements entrants. S'il n'est pas possible de diminuer votre délai d'aller-retour, il est recommandé d'envisager l'utilisation d'Adaptive Log Exporter ou de Snare. Pour plus d'informations sur Adaptive Log Exporter, voir le guide d'utilisation Adaptive Log Exporter.

Configurer le protocole Microsoft Windows Security Event Log

Pour configurer le protocole Microsoft Security Event Log, définissez les valeurs des paramètres suivants :

Tableau 1-14 Paramètres de protocole Microsoft Security Event Log

Paramètre	Description
Log Source Identifier	Saisissez l'adresse IP ou le nom d'hôte de l'hôte Windows. L'identificateur de source de journal doit être unique pour le type de source de journal.
Domain	Entrez le domaine Windows qui inclut la machine Windows spécifiée ci-dessus. Ce paramètre est facultatif.
User Name	Entrez le nom d'utilisateur requis pour accéder à l'hôte Windows.
Password	Entrez le mot de passe requis pour accéder à l'hôte Windows.
Confirm Password	Confirmez le mot de passe requis pour accéder à l'hôte Windows.
Standard Log Types	Cochez toutes les cases pour le type de journal Windows que vous souhaitez surveiller par QRadar. Au moins une case doit être cochée. Les types de journaux incluent : • Security • System • Application • DNS Server • File Replication Service • Directory Service
Event Types	Cochez les cas du type d'événement que vous souhaitez que QRadar surveille. Au moins une case doit être cochée. Les types d'événement incluent : • Informational • Avertissement • Error • Success Audit • Failure Audit

Microsoft Security Event Log Custom

Le protocole Microsoft Security Event Log fournit une collection de journaux d'événement dépourvue d'agent Windows de fichiers personnalisés EVT via l'interface de programme d'application Microsoft Windows Management Instrumentation (WMI).

Systèmes d'exploitation pris en charge

QRadar prend en charge l'interface de programme d'application Microsoft Windows Management Instrumentation suivant (WMI) :

- Microsoft Windows 2000
- Microsoft WIndows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R2
- Microsoft Windows XP
- Microsoft WIndows Vista
- Microsoft Windows 7

Types d'événements pris en charge

Le protocole Microsoft Security Event Log Custom peut traiter les fichiers historiques Windows EVT et est utilisé conjointement avec le gestionnaire universel de services de données Universal. Pour obtenir des informations sur la configuration de fichiers personnalisés EVT avec des événements pour votre système d'exploitation Windows, consultez votre documentation Microsoft.

Avant de commencer

Vous devez configurer votre pare-feu pour accepter les communications externes entrantes sur le port 135 et tous les ports dynamiques, requis pour DCOM. Pour plus d'informations sur la configuration de DCOM, voir la documentation de Microsoft Support.

Les limites suivantes de la source de journal s'appliquent lors du déploiement du protocole Microsoft Security Event Log Custom dans votre environnement :

- Une installation unique de QRadar peut prendre en charge plus de 250 sources de journal à l'aide du protocole Microsoft Security Event Log.
- Un collecteur d'événement dédié peut prendre en charge plus de 500 sources de journal à l'aide du protocole Microsoft Security Event Log.

Remarque : Le protocole Microsoft Security Event Log Custom n'est pas recommandé pour les serveurs distants, accessibles sur des liens réseau présentant des délais d'aller-retour très élevés, tel que le satellite ou les réseaux WAN lents. Le délai d'aller-retour peut être confirmé en examinant le temps de demande et de réponse entre les serveurs à l'aide de la commande PING. Les délais de réseau créés par des connexions lentes diminuent le débit ESP disponible sur ces serveurs distants. Par ailleurs, la collecte d'événements à partir de serveurs occupés ou de contrôleurs de domaine s'effectue en fonction des délais faibles d'aller-retour afin de tenir compte des événements entrants. S'il n'est pas possible de diminuer votre délai d'aller-retour, il est recommandé d'envisager l'utilisation d'Adaptive Log Exporter ou de Snare. Pour plus d'informations sur Adaptive Log Exporter, voir le document *Adaptive Log Exporter - Guide d'utilisation*.

Configurer le protocole Microsoft Windows Security Event Log Custom

Pour configurer le protocole Windows Event Log Custom, définissez les valeurs pour les paramètres suivants :

Tableau 1-15 Paramètres de protocole Windows Event Log Custom

Paramètre	Description
Log Source Identifier	Entrez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement Windows. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Domain	Entrez le domaine Windows qui inclut la machine Windows spécifiée ci-dessus. Ce paramètre est facultatif.
User Name	Entrez le nom d'utilisateur requis pour accéder à l'hôte Windows.
Password	Entrez le mot de passe requis pour accéder à l'hôte Windows.
Confirm Password	Confirmez le mot de passe requis pour accéder à l'hôte Windows.
Monitored Event Logs	Entrez le nom affiché des journaux d'événements Windows que vous souhaitez traiter. Entrez plusieurs journaux d'événements dans une liste séparée par des virgules.
Event Types	Cochez les cas du type d'événement que vous souhaitez que QRadar surveille. Au moins une case doit être cochée. Les types d'événement incluent : • Informational • Avertissement • Error • Success Audit • Failure Audit

Microsoft Exchange

Le protocole Microsoft Windows Exchange prend en charge SMTP, OWA et les journaux de suivi de messages pour Microsoft Exchange.

Pour les instructions de configuration les plus récentes, voir le *IBM Security QRadar Guide de configuration DSM.*

Le protocole Microsoft Exchange ne prend pas en charge Microsoft Exchange 2003 ou le protocole d'authentification NTLMv2 Session de Microsoft.

Remarque : Les paramètres qui prennent en charge les chemins d'accès aux fichiers vous permettent de définir un identificateur d'unité à l'aide des informations du chemin d'accès. Par exemple, vous pouvez utiliser **`c$/LogFiles/`** pour un partage administratif ou **`LogFiles/`** pour un chemin de dossier de partage public et non **`c:/LogFiles`**.

Remarque : Si un chemin de dossier de journal contient un partage administratif (C$), les utilisateurs possdéant un accès à NetBIOS sur le partage administratif (C$) disposent de leur propre accès, requis pour lire les fichiers journaux. Les administrateurs de domaine ou locaux possèdent des droits suffisants pour accéder aux fichiers journaux qui se trouvent sur les partages d'administration. La suppression des informations d'accès aux fichiers à partir de n'importe quelle zone du chemin de dossier désactive la surveillance pour ce type de journal.

Pour configurer le protocole Windows Exchange, définissez les valeurs des paramètres suivants :

Tableau 1-16 Paramètres de protocole Microsoft Exchange

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement Windows Exchange. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Server Address	Entrez l'adresse IP du serveur Microsoft Exchange.
Domain	Entrez le nom de domaine requis pour accéder au serveur Microsoft Exchange. Ce paramètre est facultatif.
Username	Entrez le nom d'utilisateur requis pour accéder au serveur Microsoft Exchange.
Password	Entrez le mot de passe requis pour accéder au serveur Microsoft Exchange.
Confirm Password	Confirmez le mot de passe requis pour accéder au serveur Microsoft Exchange.

Tableau 1-16 Paramètres de protocole Microsoft Exchange (suite)

Paramètre	Description
SMTP Log Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux SMTP. Le chemin par défaut est le suivant : **`Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/.`** La désélection des informations du chemin d'accès au fichier du champ SMTP Log Folder Path désactive la surveillance de SMTP.
OWA Log Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux OWA. Le chemin par défaut est le suivant : **`Windows/system32/LogFiles/W3SVC1`**. La désélection des informations du chemin d'accès au fichier du champ OWA Log Folder Path désactive la surveillance d'OWA.
MSGTRK Log Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux du traçage de message. Le chemin d'accès par défaut est le suivant : **`/Program Files/Microsoft /Exchange Server/TransportRoles/Logs/ MessageTracking/`** Le traçage de message est uniquement disponible sur les serveurs Microsoft Exchange 2007 affectés au rôle de serveur Hub Transport, Mailbox ou Edge Transport.
File Pattern	Entrez l'expression régulière (regex) requise pour filtrer les noms de fichiers. Tous les fichiers correspondants sont inclus dans le traitement. Le nom par défaut est le suivant.**`*\.(?:log|LOG)`** Par exemple, pour lister tous les fichiers commençant par le mot log, suivi d'un ou de plusieurs chiffres et se terminant par tar.gz, utilisez l'entrée suivante : log[0-9]+\.tar\.gz. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Force File Read	Sélectionnez cette case pour forcer le protocole à lire le fichier journal. Par défaut, la case est cochée. Si la case est désélectionnée, le fichier journal est lu lorsque ce dernier modifie l'heure ou attribut une modification à la taille du fichier.
Recursive	Cochez la case si vous souhaitez que le masque de fichiers recherche les sous-dossiers. Par défaut, la case est cochée.
Polling Interval (in seconds)	Saisissez l'intervalle d'interrogation qui correspond au nombre de secondes entre les interrogations et les fichiers journaux pour rechercher de nouvelles données. L'intervalle d'interrogation minimum est de 10 secondes, avec un intervalle d'interrogation maximum de 3600 secondes. La valeur par défaut est de de 10 secondes.

Tableau 1-16 Paramètres de protocole Microsoft Exchange (suite)

Paramètre	Description
Throttle Events/Sec	Entrez le nombre maximum d'événements que le protocole Microsoft Exchange envoie par seconde. La valeur minimale est 100 EPS et le maximum est de 20 000 EPS. La valeur par défaut est de 100 EPS.

Microsoft DHCP

Le protocole Microsoft DHCP prend uniquement en charge une connexion unique à un serveur Microsoft DHCP.

Le protocole d'authentification NTLMv2 Session de Microsoft n'est pas pris en charge dans la source de journal Microsoft DHCP. Pour configurer le protocole Microsoft DHCP, définissez les valeurs des paramètres suivants :

Tableau 1-17 Paramètres de protocole Microsoft DHCP

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement Microsoft DHCP. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Server Address	Entrez l'adresse IP du serveur Microsoft DHCP.
Domain	Entrez le nom de domaine requis pour accéder au serveur Microsoft DHCP. Ce paramètre est facultatif.
Username	Entrez le nom d'utilisateur requis pour accéder au serveur Microsoft DHCP.
Password	Entrez le mot de passe requis pour accéder au serveur Microsoft DHCP.
Confirm Password	Confirmez le mot de passe requis pour accéder au serveur Microsoft DHCP.
Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux DHCP. Le chemin par défaut est **`/WINDOWS/system32/dhcp/.`** Les utilisateurs disposant ayant un accès NetBIOS sur le partage administratif (C$) disposent de l'accès correct pour lire les fichiers journaux DHCP **`/WINDOWS/system32/dhcp/.`** Les administrateurs locaux ou les administrateurs de domaine ont des assez de privilèges pour accéder aux fichiers journaux DHCP.

Tableau 1-17 Paramètres de protocole Microsoft DHCP (suite)

Paramètre	Description
File Pattern	Entrez l'expression régulière (regex) requise pour filtrer les noms de fichiers. Tous les fichiers correspondants sont inclus dans le traitement. ***Remarque :*** *Vos fichiers suivi de journal d'audit Microsoft DHCP doit contenir une abréviation de trois caractères d'un jour de la semaine.* Le masque de fichiers IPv4 par défaut est : **`DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`** Facultatif. Masque de fichiers IPv6 : **`DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`** Facultatif. Masque de fichiers IPv4 et IPv6 : **`Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`** L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Recursive	Cochez la case si vous souhaitez que le masque de fichiers recherche les sous-dossiers. Par défaut, la case est décochée.
Polling Interval (in seconds)	Saisissez l'intervalle d'interrogation qui correspond au nombre de secondes entre les interrogations et les fichiers journaux pour rechercher de nouvelles données. L'intervalle d'interrogation minimum est de 10 secondes, avec un intervalle d'interrogation maximum de 3600 secondes. La valeur par défaut est de de 10 secondes.
Throttle Events/Sec	Entrez le nombre maximum d'événements que le protocole Microsoft DHCP envoie par seconde. La valeur minimale est 100 EPS et le maximum est de 20 000 EPS. La valeur par défaut est de 100 EPS.

Microsoft IIS

Le protocole Microsoft IIS prend en charge une collection de point unique de fichiers historiques de format.w3c depuis des serveurs Web Microsoft IIS.

Avant de commencer

Le protocole d'authentification NTLMv2 Session de Microsoft n'est pas pris en charge dans le protocole Microsoft IIS.

Configurer le protocole Microsoft IIS

Pour configurer le protocole Microsoft IIS, définissez les valeurs des paramètres suivants :

Tableau 1-18 Paramètres de protocole Microsoft IIS

Parameter	Description
Log Source Identifier	Entrez l'adresse IP, le nom d'hôte ou le nom pour identifier la source d'événements Microsoft IIS. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Server Address	Entrez l'adresse IP du serveur Microsoft IIS.
Username	Entrez le nom d'utilisateur requis pour accéder au serveur Microsoft IIS.
Password	Entrez le mot de passe requis pour accéder au serveur Microsoft IIS.
Confirm Password	Confirmez le mot de passe requis pour accéder au serveur Microsoft IIS.
Domain	Entrez le nom de domaine requis pour accéder au serveur Microsoft IIS.
Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux IIS. Le chemin d'accès par défaut est **`/WINDOWS/system32/LogFiles/W3SVC1/.`** Les paramètres qui prennent en charge les chemins de fichier vous permettent de définir un identificateur avec les informations sur le chemin. Par exemple, vous pouvez utiliser **`c$/LogFiles/`** pour un partage administratif ou **`LogFiles/`** pour un chemin de dossier de partage public mais non **`c:/LogFiles`**. Si un chemin de dossier de journal contient un partage administratif (C$), les utilisateurs possédant un accès NETBIOS sur le partage administratif (C$) possèdent l'accès requis pour lire les fichiers journaux. Les administrateurs de domaine ou locaux possèdent des droits suffisants pour accéder aux fichiers journaux qui se trouvent sur les partages d'administration.
File Pattern	Entrez l'expression régulière (regex) requise pour filtrer les noms de fichiers. Tous les fichiers correspondants sont inclus dans le traitement. Le nom par défaut est le suivant **`(?:u_)?ex.*\.(?:log|LOG)`** Par exemple, pour lister tous les fichiers commençant par le mot log, suivi d'un ou de plusieurs chiffres et se terminant par tar.gz, utilisez l'entrée suivante : log[0-9]+\.tar\.gz. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Recursive	Cochez la case si vous souhaitez que le masque de fichiers recherche les sous-dossiers. Par défaut, la case est cochée.

Tableau 1-18 Paramètres de protocole Microsoft IIS (suite)

Parameter	Description
Polling Interval (s)	Saisissez l'intervalle d'interrogation qui correspond au nombre de secondes entre les interrogations et les fichiers journaux pour rechercher de nouvelles données. La valeur par défaut est de 10 secondes.

EMC VMWare

Le protocole EMC VMWare permet à QRadar de recevoir des données d'événements à partir du service Web VMWare pour les environnements virtuels.

Pour configurer le protocole EMC VMWare, définissez les valeurs des paramètres suivants :

Tableau 1-19 Paramètres de protocole VMWare

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement de la machine virtuelle. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
ESX IP	Entrez l'adresse IP du serveur VMWare.
User Name	Entrez le nom d'utilisateur requis pour accéder au serveur VMWare.
Password	Entrez le mot de passe requis pour accéder au serveur VMWare.

SMB Tail

Le protocole SMB Tail vous permet de configurer QRadar pour interroger des fichiers spécifiques sur des sources d'événement distantes.

To configure the SMB Tail protocol, define values for the following parameters:

Tableau 1-20 Paramètres de protocole SMB Tail

Paramètre	Description
Log Source Identifier	Entrez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement SMB Tail. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Server Address	Entrez l'adresse IP du serveur.
Domain	Entrez le nom de domaine requis pour accéder au serveur. Ce paramètre est facultatif.
Username	Entrez le nom d'utilisateur requis pour accéder au serveur.
Password	Entrez le mot de passe requis pour accéder au serveur.
Confirm Password	Confirmez le mot de passe requis pour accéder au serveur.

Tableau 1-20 Paramètres de protocole SMB Tail (suite)

Paramètre	Description
Log Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux. Les paramètres qui prennent en charge les chemins de fichier vous permettent de définir un identificateur avec les informations sur le chemin. Par exemple, vous pouvez utiliser **`c$/LogFiles/`** pour un partage administratif ou **`LogFiles/`** pour un chemin de dossier de partage publique mais non **`c:/LogFiles`**. Si un chemin de dossier de journal contient un partage administratif (C$), les utilisateurs possédant un accès NETBIOS sur le partage administratif (C$) possèdent l'accès requis pour lire les fichiers journaux. Les administrateurs de domaine ou locaux possèdent des droits suffisants pour accéder aux fichiers journaux qui se trouvent sur les partages d'administration.
File Pattern	Entrez l'expression régulière (regex) requise pour filtrer les noms de fichiers. Tous les fichiers correspondants sont inclus dans le traitement. Par exemple, pour lister tous les fichiers commençant par le mot log, suivi d'un ou de plusieurs chiffres et se terminant par **`tar.gz`**, utilisez l'entrée suivante : **`log[0-9]+\.tar\.gz`**. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Force File Read	Sélectionnez cette case pour forcer le protocole à lire le fichier journal. Par défaut, la case est cochée. Si la case est décochée, le fichier journal est lu seulement lorsque QRadar détecte un changement dans l'heure ou la taille du fichier modifié.
Recursive	Cochez la case si vous souhaitez que le masque de fichiers recherche les sous-dossiers. Par défaut, la case est cochée.
Polling Interval (in seconds)	Saisissez l'intervalle d'interrogation qui correspond au nombre de secondes entre les interrogations et les fichiers journaux pour rechercher de nouvelles données. L'intervalle d'interrogation minimum est de 10 secondes, avec un intervalle d'interrogation maximum de 3600 secondes. La valeur par défaut est de de 10 secondes.
Throttle Events/Sec	Entrez le nombre maximum d'événements que le protocole SMB Tail envoie par seconde. La valeur minimale est 100 EPS et le maximum est de 20 000 EPS. La valeur par défaut est de 100 EPS.

Oracle Database Listener

La source du protocole Oracle Database Listener permet à QRadar de contrôler les fichiers journaux générés depuis une base de données d'Oracle Listener.

Avant de commencer

Avant de configurer le protocole Oracle Database Listener pour intercepter le traitement des fichiers journaux, vous devez disposer du chemin de répertoire vers les fichiers journaux de la base de données Oracle Listener. Pour plus d'informations sur la configuration d'Oracle Database Listener, consultez le Guide de configuration *IBM Security QRadar DSM*.

Configurer le protocole the Oracle Database Listener

Pour configurer le protocole Oracle Database Listener, définissez les valeurs des paramètres suivant :

Tableau 1-21 Paramètres d'écoute Oracle Database Listener

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP, un nom d'hôte ou un nom pour identifier la source d'événement Oracle Database Listener. Les adresses IP ou les noms d'hôte sont recommandés puisqu'ils permettent à QRadar d'identifier un fichier journal à une source d'événement unique.
Server Address	Entrez l'adresse IP d'Oracle Database Listener.
Domain	Entrez le nom de domaine requis pour accéder à Oracle Database Listener. Ce paramètre est facultatif.
Username	Entrez le nom de domaine requis pour accéder à l'hôte qui exécute Oracle Database Listener.
Password	Entrez le mot de passe requis pour accéder à l'hôte qui exécute Oracle Database Listener.
Confirm Password	Confirmez le mot de passe requis pour accéder à Oracle Database Listener.
Log Folder Path	Saisissez le chemin de répertoire pour accéder aux fichiers journaux Oracle Database Listener.
File Pattern	Entrez l'expression régulière (regex) requise pour filtrer les noms de fichiers. Tous les fichiers correspondants sont inclus dans le traitement. Le nom de fichier par défaut est **`listener\.log`** Ce paramètre n'accepte pas le caractère générique ou les modèles de développement dans l'expression régulière. Par exemple, si vous souhaitez lister tous les fichiers commençant par le mot log, suivi d'un ou de plusieurs chiffres et se terminant par tar.gz, utilisez l'entrée suivante : log[0-9]+\.tar\.gz. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*

Tableau 1-21 Paramètres d'écoute Oracle Database Listener (suite)

Paramètre	Description
Force File Read	Sélectionnez cette case pour forcer le protocole à lire le fichier journal lorsque le temps de l'intervalle d'interrogation le spécifie. Lorsque la case est cochée, la source du fichier journal est toujours examinée lorsque l'intervalle d'interrogation le spécifie, compte non tenu de la dernière heure de modification ou de l'attribut de la taille du fichier. Lorsque la case est décochée, la source du fichier journal est examinée au niveau de l'intervalle d'interrogation si la dernière heure de modification ou les attributs de la taille du fichier ont changé.
Recursive	Cochez la case si vous souhaitez que le masque de fichiers recherche les sous-dossiers. Par défaut, la case est cochée.
Polling Interval (in seconds)	Saisissez l'intervalle d'interrogation qui correspond au nombre de secondes entre les interrogations et les fichiers journaux pour rechercher de nouvelles données. L'intervalle d'interrogation minimum est de 10 secondes, avec un intervalle d'interrogation maximum de 3600 secondes. La valeur par défaut est de 10 secondes.
Throttle Events/Sec	Entrez le nombre maximum d'événements que le protocole Oracle Database Listener envoie par seconde. La valeur minimale est 100 EPS et le maximum est de 20 000 EPS. La valeur par défaut est de 100 EPS.

Cisco Network Security Event Logging

La source de protocole Cisco Network Security Event Logging (NSEL) permet à QRadar de contrôler les flux de paquet NetFlow depuis une Cisco Adaptive Security Appliance (ASA).

Les événements NetFlow sont compactés vers QRadar pour le traitement précédant la configuration Cisco ASA Center DSM. Pour plus d'informations, voir le Guide de configuration du gestionnaire de services de données *IBM Security QRadar*.

Pour configurer le protocole Cisco NSEL, définissez les valeurs des paramètres suivants :

Tableau 1-22 Paramètres de protocole Cisco NSEL

Paramètre	Description
Log Source Identifier	Saisissez l'adresse IP ou le nom d'hôte de la source de journal.

Tableau 1-22 Paramètres de protocole Cisco NSEL (suite)

Paramètre	Description
Collector Port	Entrez le numéro du port UDP utilisé par Cisco ASA pour transférer les événements NSEL. La plage valide du paramètre Collector Port est 1 à 65535. ***Remarque :*** *QRadar utilise généralement le port 2055 pour les données d'événement NetFlow sur QRadar QFlow Collectors. Vous devez définir un port UDP différent sur votre Cisco Adaptive Security Appliance pour NetFlow à l'aide de NSEL.*

Protocole PCAP Syslog Combination

Le protocole PCAP Syslog Combination autorise les appliances Juniper Networks SRX Series à transmettre les données (PCAP) de capture de paquets d'une applicance Juniper Networks SRX à QRadar.

Les données de capture de paquets sont transmises sur un port spécifié qui est séparé des données de syslog transférées vers QRadar sur le port 514. Les données contenues dans la capture et le port sortant depuis Juniper Networks série SRX sont configurées à partir de l'interface utilisateur du dispositif Juniper Networks série SRX. QRadar peut recevoir en même temps syslog et les données PCAP supplémentaires après avoir configuré le dispositif Juniper Networks série SRX. Pour plus d'informations sur Configuring Packet Capture, consultez votre documentation Juniper Networks JunOS.

Remarque : Votre système QRadar doit être en cours d'exécution de la dernière version de Juniper JunOS Platform DSM afin de recevoir les données PCAP depuis une appliance Juniper Networks SRX Series.

Pour configurer le protocole Juniper Networks SRX PCAP, entrez les valeurs des paramètres suivants :

Tableau 1-23 Paramètres de protocole PCAP Syslog Combination

Paramètre	Description
Log Source Identifier	Spécifiez l'adresse IP ou le nom d'hôte de la source de journal. L'adresse de l'identifiant doit être le dispositif Juniper SRX qui transfert les événements PCAP.

Tableau 1-23 Paramètres de protocole PCAP Syslog Combination (suite)

Paramètre	Description
Incoming PCAP Port	Spécifie le numéro de port utilisé par le dispositif Juniper Networks SRX Series pour transférer des données PCAP entrants vers QRadar. Le numéro de port UDP doit être configuré à partir de votre dispositif Juniper SRX Series. Si vous éditez le port PCAP sortant sur votre appareil Juniper Networks SRX Series, vous devez éditer la source de journal. Pour éditer la source du numéro de port entrant PCAP : **1** Dans le champ **Incoming PCAP Port**, entrez le nouveau numéro de port pour recevoir les données PCAP. **2** Cliquez sur **Save**. **3** Dans l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**. ***Remarque :*** *Lorsque vous cliquez sur Deploy Full Configuration, QRadar redémarre tous les services. Il en résulte un écart dans la collecte des données pour les événements et les flux jusqu'à la fin du déploiement.*

Pour plus d'informations sur le syslog pour JunOS ou Juniper Networks SRX Series, consultez le Guide de configuration du gestionnaire de services de données *IBM Security QRadar*. Pour plus d'informations sur l'affichage des données PCAP dans QRadar, voir *IBM Security QRadar - Guide d'administration*.

Protocole transféré

Le protocole transféré vous permet de recevoir une source de journal transférée depuis QRadar Console dans votre déploiement.

Le protocole est généralement utilisé dans un scénario où vous souhaitez transférer une source de journal vers une autre console QRadar. Dans ce scénario, la Console A est configuré avec une cible hors site dans l'éditeur de déploiement, qui est dirigé vers la Console B. Les sources du journal qui sont automatiquement reconnues dans QRadar sont automatiquement ajoutées vers la Console B. Toutes les sources de journal de la Console A qui sont automatiquement reconnues doivent être ajoutées à la Console B en sélectionnant **Forwarded** dans la zone de liste **Protocol Configuration**. Ceci permet à la Console B de connaître les événements de la source du journal, reçus depuis une autre Console. Par exemple, voir **Figure 1-1**.

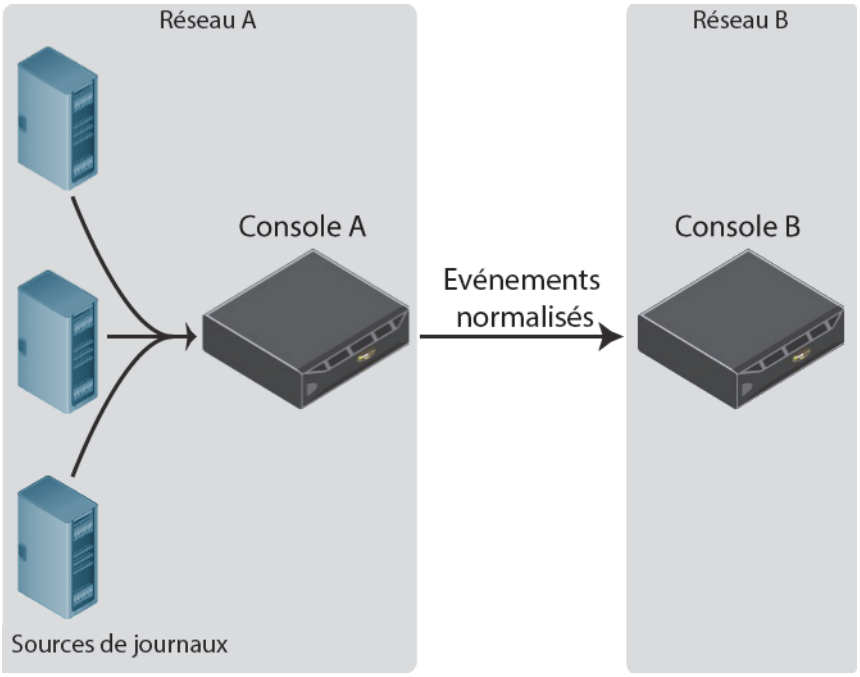

Figure 1-1 La console B reçoit des événements transférés à partir de la console A.

Dans la plupart des cas, les sources du journal qui sont automatiquement reconnues sont ajoutées à la Console B sans avoir recours à la configuration manuelle d'une source de journal. Cependant, si vous disposez d'une source de journal n'ayant aucune reconnaissance automatique, vous devez configurer manuellement la Console B pour recevoir la source de journal transférée.

Procédure

Etape 1 Connectez-vous à la console QRadar recevant des événements transférés.

Etape 2 Cliquez sur l'onglet **Admin**.

Etape 3 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 4 Cliquez sur l'icône **Log Sources**.

Etape 5 Cliquez sur **Add**.

Etape 6 Dans la zone de liste **Log Source Type**, sélectionnez un type de source de journal.

Etape 7 Dans la zone de liste **Protocol Configuration**, sélectionnez **Forwarded**.

Etape 8 Configurez les valeurs suivantes :

Tableau 1-24 Paramètres de protocole Forwarded

Parameter	Description
Log Source Identifier	Entrez une adresse IP ou un nom d'hôte pour originating log source. Par exemple, l'adresse IP ou le nom d'hôte de la source de journal dans Network A.

Etape 9 Cliquez sur **Save**.

Etape 10 Répétez les **Etape 5** à **Etape 9** pour toutes les autres sources non reconnues automatiquement dans QRadar.

Etape 11 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

La configuration de reception d'événements transférés est terminée. Pour plus d'informations sur la configuration d'une cible hors site dans l'éditeur de déploiement, voir le document*IBM Security QRadar - Guide d' administration*.

Protocole TLS Syslog

Le protocole TLS permet à QRadar de recevoir les événements de syslog chiffrés depuis plus de 50 unités réseau qui prennent en charge la transmission d'événements TLS Syslog.

Une fois la source de journal initiale TLS Syslog créée et le port d'écoute pour le syslog configuré pour le syslog TLS, QRadar génère un certificat de syslog-tlsa. Ce certificat peut être copié vers tout périphérique réseau capable de transférer le protocole syslog chiffré. Les périphériques réseau supplémentaires avec le fichier certificat syslog-tls et le numéro du port d'écoute TLS peuvent être automatiquement reconnus comme source de journal TLS syslog dans QRadar.

Remarque : Votre périphérique réseau peut exiger la configuration supplémentaire après la copie du certificat pour activer le transmission d'événements TLS Syslog. Pour plus d'informations, voir la documentation de votre fournisseur.

Pour configurer le protocole TLS Syslog, vous devez :

1. Installez le protocole TLS Syslog.
2. Créez une source de journal TLS Syslog.
3. Copiez le certificat TLS Syslog vers votre périphérique réseau.

Création d'une source de journal TLS Syslog

Avant que QRadar puisse accepter les événements syslog chiffrés entrants d'un périphérique réseau, vous devez créer une source de journal qui utilise le protocole TLS Syslog. La création de la source de journal permet à QRadar d'établir un port pour les événements pour les événements entrants TLS Syslog et de générer un fichier certificat pour vos périphériques réseau. Toute source de journal qui prend en charge le protocole syslog comprend également une option de configuration de protocole pour TLS Syslog, mais tous les périphériques réseau ne peuvent pas transférer des événements TLS Syslog vers QRadar.

Remarque : Pour déterminer si votre périphérique prend en charge TLS Syslog, voir la documentation du fournisseur de votre périphérique réseau.

Procédure

Etape 1 Connectez-vous à QRadar.

Etape 2 Cliquez sur l'onglet **Admin**.

Etape 3 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 4 Cliquez sur l'icône **Log Sources**.

Etape 5 Cliquez sur **Add**.

Etape 6 Dans la zone **Log Source Name**, entrez un nom pour votre source de journal.

Etape 7 Dans la zone **Log Source Description,** entrez une description pour votre source de journal.

Etape 8 Dans la zone de liste **Log Source Type**, sélectionnez un type de source de journal prenant en charge le chiffrement de syslog TLS.

Etape 9 Dans la zone de liste **Protocol Configuration**, sélectionnez **TLS Syslog**.

Etape 10 Configurez les valeurs suivantes :

Tableau 1-25 Paramètres de protocole Forwarded

Paramètre	Description
Log Source Identifier	Saisissez l'adresse IP ou le nom d'hôte de l'appareil réseau qui transmet le syslog chiffré.

Tableau 1-25 Paramètres de protocole Forwarded (suite)

Paramètre	Description
TLS Listen Port	Entrez le numéro de port utilisé par QRadar pour accepter les événements entrants TLS Syslog. L'intervalle de port valide est 1 à 65536. La valeur par défaut du port d'écoute TLS est 6514. Le numéro de port indiqué comme port d'écoute pour les événements TLS peut être utilisé par plus de 50 sources de journal. Si plusieurs périphériques réseau transmettent des événements TLS syslog, ils peuvent également utiliser 6514 comme leur port TLS syslog par défaut. ***Remarque :*** *Si vous ne voyez pas le champ TLS Listen Port, vous devez redémarrer Tomcat sur QRadar. Pour plus d'informations, voir* **Installation manuelle d'un protocole de source de journal**,**Etape 8**. Pour éditer la source du numéro de port entrant TLS Listen : **1** Dans le champ **Incoming TLS Listen Port**, entrez le numéro de port pour recevoir les événements TLS syslog. **2** Cliquez sur **Save**. **3** Dans l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**. ***Remarque :*** *Lorsque vous cliquez sur Deploy Full Configuration, QRadar redémarre tous les services. Il en résulte un écart dans la collecte des données pour les événements et les flux jusqu'à la fin du déploiement.*

Etape 11 Cliquez sur **Save**.

Etape 12 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Après avoir créé votre source de journal TLS Syslog, vous devez copier le certificat TLS à partir de QRadar vesr votre périphérique réseau en fournissant les événements TLS Syslog.

Copie du certificat TLS Syslog

Après avoir configuré une source de journal TLS Syslog, QRadar crée un fichier certificat générique syslog-tls qui peut être utilisé avec plusieurs périphériques réseau, capables de transmettre le protocole syslog chiffré.

Procédure

Etape 1 A l'aide de Secure Shell, connectez-vous à QRadar en tant que superutilisateur.

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Etape 2 Accédez au répertoire de certificats de confiance dans QRadar.

`/opt/qradar/conf/trusted_certificates/`

Etape 3 Ce répertoire contient les deux fichiers syslog suivants :

- **syslog-tls.cert** - Le fichier de certificat que vous copiez vers vos périphériques réseau afin qu'ils puissent communiquer avec QRadar.
- **syslog-tls.key** - Le fichier clé privé permettant aux périphériques réseau de communiquer avec QRadar. Ce fichier n'a pas été entièrement copié.

Etape 4 Copiez le fichier syslog-tls.cert vers votre périphérique réseau.

Le chemin de répertoire des fichiers certificat varie entre les périphériques réseau. Pour déterminer le chemin de certificat adéquat, voir la documentation du fournisseur de votre périphérique réseau.

La configuration TLS Syslog pour QRadar est terminée.

Une fois qu'une source de journal TLS Syslog a été créée et déployée, celle-ci génère un certificat de syslog-tls, les autres unités peuvent être configurées pour l'envoi des événements vers le même port utilisant le même certificat. Les sources de journal sont créées automatiquement pour les flux d'événement envoyés vers le port d'écoute TLS Syslog lorsque la source du journal prend en charge la reconnaissance automatique. Le nombre maximum de sources de journal TLS Syslog qui peuvent être associées à un seul port d'écoute TLS est limité à 50. Pour ajouter davantage de sources de journal après les 50 premières, vous devez définir que les sources de journal complémentaires utilisent un numéro de port d'écoute différent. Vous pouvez ensuite configurer vos unités afin qu'elles transfèrent les événements de vos sources de journal complémentaires vers l'autre port d'écoute TLS.

Protocole Juniper Security Binary Log Collector

QRadar peut accepter les événements d'audit, du système, du pare-feu et du système de prévention contre les intrusions (SIP) dans le format binaire des appliances Juniper SRX ou Juniper Networks J Series.

Le format binaire du fichier de journal Juniper Networks est destiné à améliorer la performance pendant l'écriture des gros volumes de données vers un journal d'événement. Pour intégrer votre unité, vous devez configurer votre appliance Juniper pour compacter les événements binaires formatés puis configurez une source de journal dans QRadar. Le format de journal binaire des dispositifs Juniper SRX ou J sont transférés vers QRadar à l'aide du protocole UDP. Vous devez spécifier un port unique pour la diffusion d'événements formatés, le port du syslog standard pour QRadar ne peut pas contenir des événements binaires formatés. Le port par défaut affecté à QRadar pour la réception d'événements binaires de transmission à partir des dispositifs Juniper est le port 40798.

Pour obtenir des informations sur la configuration de votre appliance Juniper SRX or J Series, consultez la section du Guide de configuration du gestionnaire de services de données Juniper Security Binary Log Collect*IBM Security QRadar*.

Configuration du protocole Juniper Binary Log Collector

Pour configurer une source de journal afin que votre Juniper Security Binary Log Collector collecte des événements binaires à haute vitesse.

Procédure

Etape 1 Connectez-vous à QRadar.

Etape 2 Cliquez sur l'onglet **Admin**.

Etape 3 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 4 Cliquez sur l'icône **Log Sources**.

Etape 5 Cliquez sur **Add**.

Etape 6 Dans la zone **Log Source Name**, entrez un nom pour votre source de journal.

Etape 7 Dans la zone **Log Source Description,** entrez une description de la source de journal.

Etape 8 Dans la zone de liste **Log Source Type**, sélectionnez **Juniper Security Binary Log Collector**.

Etape 9 A l'aide de la zone de liste **Protocol Configuration**, sélectionnez **Juniper Security Binary Log Collector**.

Etape 10 Configurez les valeurs suivantes :

Tableau 1-26 Paramètres de protocole Juniper Security Binary Log Collector

Paramètre	Description
Log Source Identifier	Saisissez une adresse IP ou un nom d'hôte pour identifier la source de journal. L'adresse de l'identifiant doit être le dispositif Juniper SRX ou J Series qui génère le flux d'événements binaires.

Tableau 1-26 Paramètres de protocole Juniper Security Binary Log Collector (suite)

Paramètre	Description
Binary Collector Port	Spécifie le numéro de port utilisé par le dispositif Juniper Networks SRX Series ou J Series pour transférer les données binaires entrants vers QRadar. Pour plus d'informations sur la configuration des ports pour votre appliance Juniper SRX Series ou Juniper J Series, voir le Guide de configuration *IBM Security QRadar DSM*. Si vous éditez le numéro de port sortant pour le flux d'événements binaires sur votre dispositif Juniper Networks SRX ou J Series, vous devez également éditer votre source de journal Juniper et mettre à jour le paramètre **Binary Collector Port** dans QRadar. Pour éditer le port : **1** Dans le champ **Binary Collector Port**, entrez le numéro de port pour recevoir les données d'événements binaires. **2** Cliquez sur **Save**. La collection d'événements est arrêtée pour la source de journal qu'au déploiement total de QRadar. **3** Dans l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**. La mise à jour du port est terminée et la collecte d'événements démarre sur le nouveau numéro de port. ***Remarque :*** *Lorsque vous cliquez sur Deploy Full Configuration, QRadar redémarre tous les services. Il en résulte un écart dans la collecte des données pour les événements et les flux jusqu'à la fin du déploiement.*
XML Template File Location	Entrez le chemin d'accès fichier XML utilisé pour décoder le flux binaire sur votre dispositif Juniper SRX ou Juniper J Series. Par défaut, QRadar inclut un XML pour décoder le flux binaire dans le répertoire suivant : **`/opt/qradar/conf/security_log.xml`**

Etape 11 Cliquez sur **Save**.

Etape 12 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

Protocole UDP Multiline Syslog

QRadar peut accepter des messages d'événement syslog multiligne UDP à partir d'une source d'événement capable d'envoyer un message d'événement dans un format syslog multiligne qui contient une valeur d'identification commune sur chaque ligne du message d'événement.

Le protocole syslog multiligne UDP utilise une expression régulière dans la zone **Message ID Pattern** pour identifier et réassembler les messages syslog multiligne dans une charge utile d'événement unique pour QRadar.

Par exemple, l'exemple de texte suivant utilise un numéro de connexion qui peut être utilisé en tant que modèle de message pour réassembler l'événement dans une seule charge utile pour QRadar:

15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com”

Configurez le protocole UDP Multiline Syslog

Vous pouvez configurer le protocole UDP Multiline Syslog pour collecter des événements pour QRadar qui étendent plusieurs lignes.

Procédure

Etape 1 Connectez-vous à QRadar.

Etape 2 Cliquez sur l'onglet **Admin**.

Etape 3 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 4 Cliquez sur l'icône **Log Sources**.

Etape 5 Cliquez sur **Add**.

Etape 6 Dans la zone **Log Source Name**, entrez un nom pour votre source de journal.

Etape 7 Dans la zone **Log Source Description**, entrez une description pour votre source de journal.

Etape 8 Dans la zone de liste **Log Source Type**, sélectionnez un type de source de journal qui prend en charge les messages d'événement syslog multiligne UDP.

Etape 9 Dans la zone de liste **Protocol Configuration**, sélectionnez **UDP Multiline Syslog**.

Etape 10 Configurez les valeurs suivantes :

Tableau 1-27 Paramètres de protocole UDP Multiline

Paramètre	Description
Log Source Identifier	Entrez une adresse IP, un nom d'hôte ou un nom pour identifier la source de journal ou l'appliance fournissant les événements UDP Multiline Syslog vers QRadar.

Tableau 1-27 Paramètres de protocole UDP Multiline (suite)

Paramètre	Description
Listen Port	Entrez le numéro de port utilisé par QRadar pour accepter les événements entrants UDP Multiline Syslog. La plage de ports valide est 1 et 65535. La valeur par défaut du port UDP Multiline Syslog listen est 517. ***Remarque :*** *Si vous ne voyez pas le champ Listen Port, vous devez redémarrer Tomcat sur QRadar. Pour plus d'informations, voir* **Installation manuelle d'un protocole de source de journal**,**Etape 8**. Pour éditer le numéro de port d'écoute : **1** Mettez à jour IPtables sur votre console ou collecteur d'événements QRadar avec le nouveau numéro de port UDP Multiline Syslog. Pour plus d'informations, voir la section Open LDAP du Guide de configuration *IBM Security QRadarDSM.* **2** Dans le champ **Listen Port**, entrez le numéro de port pour recevoir les événements UDP Multiline Syslog. **3** Cliquez sur **Save**. **4** Dans l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**. ***Remarque :*** *Lorsque vous cliquez sur Deploy Full Configuration, QRadar redémarre tous les services. Il en résulte un écart dans la collecte des données pour les événements et les flux jusqu'à la fin du déploiement.*
Message ID Pattern	Entrez l'expression régulière (regex) requise pour filtrer les messages de données utiles. Tous les événements correspondants sont inclus lors du traitement des événements Open LDAP. Par exemple, l'expression régulière suivante peut être utilisée pour analyser les événements syslog multiligne UDP pour Open LDAP : `conn=(\d+)` L'expression régulière requise peut être différente selon les événements multiligne générés par votre unité ou votre dispositif. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*

Etape 11 Cliquez sur **Save**.

Etape 12 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

La configuration est terminée.

TCP Multiline Syslog Protocole

QRadar peut accepter les messages d'événements multi-lignes du syslog TCP TCP à partir de n'importe quelle source capable d'envoyer un message d'événement dans un format multi-lignes de syslog.

Le protocole TCP Multiline Syslog exige un motif d'expression régulière pour identifier le démarrage, l'arrêt ou à la fois le motif de démarrage ou d'arrêt de l'événement à analyser. Ceci permet au protocole d'identifier là où démarre ou se termine un événement pour rassembler avec exactitude la charge utiled'événements multi-lignes en une charge unique d'événements pour QRadar.

Par exemple, l'événement suivant démarre toujours avec un horodatage pour chaque message de syslog TCP. TCP Multiline Syslog Protocol peut utiliser un motif d'expression régulière pour l'horodatage afin d'identifier un événement individuel. Le protocole recueille les informations après l'horodatage initial et rassemble les événements dans une charge utile unique pour QRadar.

```
06/13/2012 20:15:15
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

Configuration du protocole TCP Multiline Syslog

Vous pouvez configurer le protocole TCP Multiline Syslog pour collecter des événements pour QRadar qui sont au format TCP multiline.

Procédure

Etape 1 Connectez-vous à QRadar.

Etape 2 Cliquez sur l'onglet **Admin**.

Etape 3 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 4 Cliquez sur l'icône **Log Sources**.

Etape 5 Cliquez sur **Add**.

Etape 6 Dans la zone **Log Source Name**, entrez un nom pour votre source de journal.

Etape 7 Dans la zone **Log Source Description,** entrez une description pour votre source de journal.

Etape 8 Dans la zone de liste **Log Source Type**, sélectionnez un type de source de journal qui prend en charge les messages d'événement syslog multiligne UDP.

Etape 9 Dans la zone de liste **Protocol Configuration**, sélectionnez **TCP Multiline Syslog**.

Etape 10 Configurez les valeurs suivantes :

Tableau 1-28 Paramètres de protocole TCP Multiline

Paramètre	Description
Log Source Identifier	Entrez une adresse IP, un nom d'hôte ou un nom pour identifier la source de journal ou l'appliance fournissant les événements TCP Multiline Syslog à QRadar.
Listen Port	Entrez le numéro de port utilisé par QRadar pour accepter les événements TCP Multiline Syslog entrants. La plage de ports valide est 1 et 65535. Le port d'écoute TCP Multiline par défaut est de 12468. ***Remarque :*** *Si vous ne voyez pas le champ Listen Port, vous devez redémarrer Tomcat sur QRadar. Pour plus d'informations, voir* **Installation manuelle d'un protocole de source de journal**,**Etape 8**. Pour éditer le numéro de port d'écoute : Dans le champ **Listen Port,** entrez le nouveau numéro de port **1** pour la réception d'événements TCP Multiline Syslog. **2** Cliquez sur **Save**. **3** Dans l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration**. ***Remarque :*** *Lorsque vous cliquez sur Deploy Full Configuration, QRadar redémarre tous les services. Il en résulte un écart dans la collecte des données pour les événements et les flux jusqu'à la fin du déploiement.*
Event Formatter	Le formateur d'événements s'applique au traitement et au formatage supplémentaire aux événements multi-lignes entrants pour QRadar. Pour la zone de liste Event Formatter, sélectionnez une des options suivantes : • **No Formatting** - Aucun formatage supplémentaire ne s'applique aux événements multi-ligne entrants. • **Windows Multiline** - Les événements multi-lignes entrants sont particulièrement formatés pour les événements basés sur Windows et transmis depuis des appliances ou systèmes SIEM.

Tableau 1-28 Paramètres de protocole TCP Multiline (suite)

Paramètre	Description
Event Start Pattern	Entrez l'expression régulière (regex) requise pour identifier le démarrage d'une charge TCP d'événements multi-lignes. Par exemple, les en-têtes de syslog commencent généralement avec une date ou un horodatage. Le protocole est capable de capturer des événements basés uniquement sur un modèle de démarrage d'événement tel qu'un horodatage lorsqu'il n'existe aucun modèle d'achèvement utilisable ou répétitif. Au cas où seul un motif de démarrage serait disponible, le protocole capture toutes les informations entre chaque horodatage dans la charge multi-lignes pour créer un événement valide pour QRadar. L'expression régulière obligatoire peut être différent selon les événements TCP multi-lignes générés par votre unité ou votre appliance. L'utilisation de ce paramètre requiert la connaissance de l'expression régulière (regex). Pour plus d'informations, consultez le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*
Event End Pattern	Entrez l'expression régulière (regex) requise pour identifier le dernier champ d'une charge d'événement TCP multi-lignes. Par exemple, si vote syslog se termine généralement avec la même valeur, vous pouvez utiliser cette valeur de fin répétitive dans le champ **Event End Pattern.** Le protocole est capable de capturer des événements basés uniquement sur un motif d'événement lorsqu'il n'existe aucun motif d'arrêt utilisable ou répétitif. Au cas où seul le motif d'arrêt serait disponible, le protocole capture toutes les informations entre chaque valeur de fin dans la charge utile multi-ligne pour créer un événement valide pour QRadar. L'expression régulière obligatoire peut être différente selon les événements TCP multi-lignes générés par votre unité ou appliance. L'utilisation de ce paramètre exige la connaissance des expressions régulières (regex). Pour plus d'informations, voir le site Web suivant : *http://download.oracle.com/javase/tutorial/essential/regex/*

Etape 11 Cliquez sur **Save**.

Etape 12 Sur l'onglet **Admin**, cliquez sur **Deploy Changes**.

La configuration est terminée.

Protocole IBM Tivoli Endpoint Manager SOAP

Le protocole IBM Tivoli Endpoint Manager SOAP de QRadar extrait les événements formatés Log Extended Event Format (LEEF) d'IBM Tivoli Endpoint Manager.

QRadar utilise le protocole Tivoli Endpoint Manager SOAP pour extraire les événements sur un intervalle de 30 secondes. Au fur et à mesure que les événements sont extraits, le DSM IBM Tivoli Endpoint Manager analyse et catégorise les événements pour QRadar. L'API SOAP pour IBM Tivoli Endpoint

Manager n'est disponible qu'après installation avec l'application Web Reports. L'application Web Reports pour Tivoli Endpoint Manager est requise pour extraire et intégrer les données d'événement du système IBM Tivoli Endpoint Manager avec QRadar.

Remarque : QRadar est compatible avec IBM Tivoli Endpoint Manager versions 8.2.x. Toutefois, nous vous recommandons d'effectuer une mise à jour vers la dernière version d'IBM Tivoli Endpoint Manager disponible.

Tableau 1-29 Paramètres de protocole IBM Tivoli Endpoint Manager SOAP

Paramètre	Description
Log Source Identifier	Saisissez l'adresse IP ou le nom d'hôte de votre dispositif IBM Tivoli Endpoint Manager. L'adresse IP ou le nom d'hôte identifie votre dispositif IBM Tivoli Endpoint Manager en tant que source d'événement unique dans QRadar.
Port SOAP	Saisissez le numéro de port utilisé pour vous connecter au dispositif IBM Tivoli Endpoint Manager à l'aide de l'API SOAP. Par défaut, le port 80 est le numéro de port autorisant la communication avec IBM Tivoli Endpoint Manager.
Username	Saisissez le nom d'utilisateur requis pour accéder à IBM Tivoli Endpoint Manager.
Password	Saisissez le mot de passe requis pour accéder à votre dispositif IBM Tivoli Endpoint Manager.
Confirm Password	Confirmez le mot de passe nécessaire pour accéder à votre dispositif IBM Tivoli Endpoint Manager.

Sources de journal groupées

Vous pouvez afficher les sources de journal basées sur la fonctionnalité. Le classement de vos sources de journal dans des groupes vous permet d'afficher et de suivre efficacement vos sources de journal. Par exemple, vous pouvez afficher toutes les sources de journal par nom. Chaque groupe peut afficher un nombre maximal de 1000 sources de journal.

Vous devez disposer d'un accès administrateur pour créer, modifier ou supprimer des groupes. Pour plus d'informations sur les rôles de l'utilisateur, voir *IBM Security QRadar - Guide d'administration.*

Affichage des sources de journal utilisant des groupes

Pour afficher des sources de journal utilisant des groupes, procédez comme suit :

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Dans la zone de liste **Search For**, sélectionnez l'option de groupe à afficher.

Etape 5 Sélectionnez vos critères de groupe.

Etape 6 Cliquez sur **Go**.

Les résultats de groupe s'affichent.

Création d'un groupe de source de journal

Pour créer un groupe, procédez comme suit :

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Groups**.

Etape 4 Dans l'arborescence du menu, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

Remarque : Par ailleurs, cliquez sur **Assign** pour accéder à l'option de menu de groupe de la source de journal.

Etape 5 Cliquez sur **New Group**.

Etape 6 Définir les valeurs pour les paramètres :

- **Nom** - Entrez un nom à affecter au nouveau groupe. Le nom peut contenir plus de 255 caractères et est sensible à la casse.
- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossiers vers un emplacement choisi dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups Properties.

Remarque : Lorsque vous créez le groupe, vous pouvez glisser-déplacer les éléments pour changer l'organisation des éléments de l'arborescence des menus.

Edition d'un groupe de sources de journal

Pour modifier un groupe, procédez comme suit :

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Groups**.

Etape 4 Dans l'arborescence du menu, sélectionnez le groupe à modifier.

Etape 5 Cliquez sur **Edit**.?

Etape 6 Mettez les valeurs des paramètres à jour, si nécessaire :

- **Nom** - Entrez un nom à affecter au nouveau groupe. Le nom peut contenir plus de 255 caractères et est sensible à la casse.
- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossiers vers un emplacement convenable dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Groups.

Copie d'une source de journal vers un autre groupe

En utilisant la fonctionnalité des groupes, vous pouvez copier une source de journal vers un ou plusieurs groupes.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Groups**.

Etape 4 Dans l'arborescence Log Source Groups, sélectionnez le groupe à partir duquel vous souhaitez copier la source de journal.

Etape 5 Dans Group Content Frame, sélectionnez la source de journal que vous souhaitez copier vers un autre groupe.

Etape 6 Cliquez sur **Copier**.

Etape 7 Sélectionnez le groupe vers lequel vous souhaitez copier la source de journal.

Etape 8 Cliquez sur **Assign Groups**.

Etape 9 Fermez la fenêtre Groups.

Suppression d'une source de journal d'un groupe

La suppression d'un groupe de la source de journal ne retire pas cette dernière de QRadar. Seule l'association de groupes est supprimée.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Groups**.

Etape 4 Dans l'arborescence du menu, sélectionnez le groupe contenant les éléments à supprimer.

Etape 5 Dans Group Content Frame, sélectionnez l'élément à supprimer.

Etape 6 Cliquez sur **Remove**.

Etape 7 Cliquez sur **OK**.

Etape 8 Fermez la fenêtre Groups.

Définition de l'ordre d'analyse syntaxique de la source de journal

Vous pouvez configurer la commande dont vous souhaitez que chaque collecteur d'événement de votre déploiement analyse les événements à partir des sources de journal DSM (Modules de services de périphériques). Si un DSM contient plusieurs sources entrantes de journal sous la même adresse IP ou le même nom d'hôte, vous devez souligner l'importance de ces sources de journal entrantes en définissant la commande d'analyse syntaxique.

La définition de la commande d'analyse syntaxique des sources de journal veille à ce que ces dernières soient analysées dans un ordre spécifique, malgré les modifications apportées à la configuration de la source de journal. Cela permet de s'assurer que les performances du système ne sont pas affectées par les modifications apportés à la configuration de la source de journal, empêchant ainsi une analyse syntaxique inutile.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Parsing Ordering.**

Remarque : Si toutes les sources de journal sont configurées pour le collecteur d'événement sélectionné, seule la zone de liste **Selected Event Collector** s'affiche.

Etape 4 Définissez les valeurs des paramètres suivants :

- **Selected Event Collector** - Dans cette zone de liste, sélectionnez Event Collector pour définir la commande d'analyse syntaxique de la source de journal.
- **Log Source Host** - Dans cette zone de liste, sélectionnez l'hôte de la source de journal qui envoie les événements vers le collecteur d'événement sélectionné.

  Si plusieurs hôtes existent sur le collecteur d'événement, la liste des hôtes disponibles s'affiche. Sélectionnez l'hôte à partir du paramètre **Filter** ou sélectionnez la liste ci-dessous.

Etape 5 Pour définir les priorités de la commande de l'analyse syntaxique de la source de journal :

a Sélectionnez la source de journal dont vous souhaitez définir les priorités.

b Définissez les priorités de l'ordre de la source de journal à l'aide des boutons disponibles :

Up - déplace la source de journal vers le haut dans la commande de l'analyse syntaxique.

Down - déplace la source de journal vers le bas dans la commande de l'analyse syntaxique.

Top - déplace la source de journal vers la partie supérieure de la commande de l'analyse syntaxique.

Bottom - déplace la source de journal vers la partie inférieure de la commande de l'analyse syntaxique.

Remarque : Pour déplacer une source de journal vers une commande spécifique dans la liste de l'analyse syntaxique, sélectionnez la source de journal, puis utilisez le paramètre **Move to**.

Etape 6 Cliquez sur **Save**.

Etape 7 Répétez toutes les sources de journal souhaitées.

2 GESTION DES EXTENSIONS DE SOURCE DE JOURNAL

Les extensions de la source de journal vous permettent d'étendre immédiatement ou de modifier les routines d'analyse d'unités spécifiques.

Par exemple, vous pouvez utiliser une extension de source de journal pour détecter un événement manquant ou des champs incorrects. Une extension de source de journal peut également analyser un événement lorsque le module de service de périphérique à qui il est rattaché ne réussit pas à produire un résultat.

Pour obtenir des informations sur la configuration des sources du journal, voir **Gestion des sources de journaux**.

Cette section fournit des informations sur l'étape suivante :

- **A propos des extensions de source de journal**
- **Création d'un document d'extension de source de journal**
- **Affichage des extensions de source de journal**
- **Ajout d'une extension de source de journal**
- **Edition d'une extension de source de journal**
- **Copie d'une extension de source de journal**
- **Suppression d'une extension de source de journal**
- **Activation ou désactivation d'une extension de source de journal**

A propos des extensions de source de journal

Une extension de source de journal permet à un module de service de périphérique d'analyser des journaux même si le module de service de périphérique n'a pas reçu une mise à jour ou le module de service de périphérique n'existe pas pour ce type de source de journal. Les informations sur les extensions de source de journal sont accessibles à partir l'onglet **Admin**.

Vous pouvez aussi créer des rapports d'extension de source de journal pouvant être envoyés au support clientèle. Cette capacité est un mécanisme de génération de rapports de problèmes lié à l'analyseet aux éventuels correctifs vers notre département de support clientèle afin qu'ils puissent être évalués pour l'inclusion des futures mises à jour DSM.

Création d'un document d'extension de source de journal

Avant de définir une extension de source de journal dans QRadar, vous devez créer le document d'extension. Le document d'extension est un document XML que vous créez ou modifiez en utilisant toute application commune de traitement de texte. Plusieurs documents d'extension peuvent être créés, téléchargés et associés à différents types de sources de journaux.

Le format du document d'extension doit être conforme à un document de schéma XML standard (XSD). Pour développer un document d'extension, une connaissance spécialisée et une expérience avec la codification XML est obligatoire.

Pour plus d'informations sur la création d'un document d'extensions, voir **Créer un document d'extensions**.

Le nom du document d'extension doit être au format suivant :

```
<filename>.xml
```

Lorsque vous sélectionnez un document d'extension pour le télécharger, QRadar approuve le document contre le XSD interne. QRadar vérifie également la validité du document avant son téléchargement vers le système. La procédure suivante est un exemple de document valide d'extension de source de journal :

```
<?xml version="1.0" encoding="UTF-8" ?>
<device-extension xmlns="event_parsing/device_extension">
  <pattern id="EventName" xmlns=""><![CDATA[
%FWSM[a-zA-Z\-]*\d-(\d{1,6}) ]]></pattern>
  <pattern id="SourceIp" xmlns=""><![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
  <pattern id="EventNameId"
xmlns=""><![CDATA[(\d{1,6})]]></pattern>
  <match-group order="1" description="FWSM Test"
device-type-id-override="6" xmlns="">
  <matcher field="EventName" order="1" pattern-id="EventName"
capture-group="1"    enable-substitutions="false" />
  <matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="1" />
  <event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Cisco Firewall"
severity="7" send-identity="OverrideAndNeverSend" />
</match-group>
</device-extension>
```

Remarque : Tous les caractères entre le <modèle> de balise ouvrante et le </modèle> de balise fermante sont considérés comme étant des composants du modèle. N'utilisez pas des espaces supplémentaires et des retours fixes ou autour de votre modèle ou expression <CDATA>. Les caractères ou espaces supplémentaires peuvent empêcher à l'extension DSM de trouver votre modèle prévu.

Affichage des extensions de source de journal

Une liste d'extensions de la source de journal, leur statut ainsi que leur description s'affichent dans la fenêtre Log Source Extensions.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Extensions**.

La fenêtre Log Source Extensions fournit les détails suivants pour chaque extension de source de journal :

Tableau 2-1 Paramètres d'extension de source de journal

Paramètre	Description
Nom d'extension	Le nom de l'extension de source de journal. Après que vous ayez ajouté une extension de source de journal, cliquez sur **Extension Name** pour télécharger le fichier xml associé à la substitution ou à l'amélioration de l'analyse.
Description	La description de l'extension de source de journal. La description doit dépasser 255 caractères.
Activée	Spécifie si l'extension de source de journal est activée (vrai) ou désactivée (faux).
Valeur par défaut pour types de source de journal	L'extension pour les types de source de journal est en cours de redéfinition ou d'amélioration. Un fichier d'extension de source de journal peut être appliqué à plusieurs sources du journal. L'analyse syntaxique de toutes les sources répertoriées du journal sont en cours d'amélioration ou ont des substitutions d'analyse déjà appliquées.

Ajout d'une extension de source de journal

Les extensions de la source de journal vous permettent d'étendre immédiatement ou de modifier les routines d'analyse d'unités spécifiques.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Extensions**.

Etape 4 Cliquez sur **Add**.

Etape 5 Configurez les valeurs des paramètres suivants :

Tableau 2-2 Ajoutez un paramètre des sources du journal

Paramètre	Description
Nom	Entrez un nom pour l'extension de source de journal. Ce nom peut contenir un nombre maximal de 255 caractères alphanumériques incluant un trait de soulignement (_).
Description	Entrez un nom pour l'extension de source de journal. La description ne peut pas être supérieure à 255 caractères.
Conditions d'utilisation	Dans la zone de liste, sélectionnez l'une des options suivantes : • **Parsing Enhancement** - Sélectionnez cette option lorsque le gestionnaire de services de données analyse correctement la plupart des zones de la source de journal mais nécessite de corriger une ou deux zones. Ces valeurs de zone incorrectes sont améliorées avec les nouvelles valeurs XML. Il s'agit du paramètre par défaut. • **Parsing Override** - Sélectionnez cette option lorsque le gestionnaire de services de données ne parvient pas à analyser correctement les informations spécifiques et requises de l'unité, ou ne parvient pas à les extraire. Cette extension de source de journal redéfinit entièrement l'analyse défectueuse via le module de service de périphérique et substitue l'analyse avec les nouvelles valeurs XML.
Types de source de journal	Sélectionnez les sources de journal à ajouter ou supprimer de l'analyse d'extension. Les options comprennent : • **Available** - Sélectionnez un type de source de journal puis cliquez sur la flèche pour ajouter la source de journal à la liste **Set to default for**. • **Set to default for** - Sélectionnez un type de source de journal et cliquez sur la flèche gauche pour supprimer un type de source de journal de la liste **Set to default for**. Répétez cette étape pour chaque type de source de journal dont vous souhaitez substituer ou améliorer l'extension.

Etape 6 Dans le champ **Upload Extension**, cliquez sur **Browse** puis localisez un document d'extension de source de journal (`<filename>.xml`) qui est téléchargé.

Etape 7 Cliquez sur **Upload**.

Les contenus du fichier d'extension s'affichent Ce contenu affiché n'est pas modifiable.

Etape 8 Cliquez sur **Save**.

La nouvelle extension de source de journal est créée. Le collecteur d'événement détecte automatiquement les changements et exécute l'extension de source de journal.

Par défaut, de nouvelles extensions de source de journal sont activées. Si vous souhaitez désactiver l'extension de source de journal, voir **Activation ou désactivation d'une extension de source de journal**.

Edition d'une extension de source de journal

Cette section fournit des informations sur la manière d'éditer une extension de source de journal, telles que la modification de la définition d'une extension de source de journal ou le changement d'unité vers l'extension de source de journal par défaut.

Pour modifier une extension de source de journal, procédez comme suit :

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Extensions**.

Etape 4 A partir de la liste d'extensions de source de journal, sélectionnez l'extension de source de journal que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

Etape 6 Modifiez vos paramètres d'extension, si nécessaire :

Tableau 2-3 Modifiez les paramètres d'extension de source de journal

Paramètre	Description
Nom	Entrez le nom pour l'extension de source de journal. Ce nom peut contenir un nombre maximal de 255 caractères alphanumériques plus le trait de soulignement (_).
Description	Entrez la description pour l'extension de source de journal. La description ne peut pas être supérieure à 255 caractères.
Conditions d'utilisation	Dans la zone de liste, sélectionnez l'une des options suivantes : • **Parsing Enhancement** - Sélectionnez cette option lorsque le gestionnaire de services de données analyse correctement la plupart des zones de la source de journal mais nécessite de corriger une ou deux zones. Ces valeurs de zone incorrectes sont améliorées avec les nouvelles valeurs XML. Il s'agit du paramètre par défaut. • **Parsing Override** - Sélectionnez cette option lorsque le gestionnaire de services de données ne parvient pas à analyser correctement les informations spécifiques et requises de l'unité, ou ne parvient pas à les extraire. Cette extension de source de journal redéfinit entièrement l'analyse défectueuse via le module de service de périphérique et substitue l'analyse avec les nouvelles valeurs XML.
Types de source de journal	Sélectionnez les sources de journal à ajouter ou supprimer de l'analyse d'extension. Les options comprennent : • **Available** - Sélectionnez un type de source de journal puis cliquez sur la flèche pour ajouter la source de journal à la liste **Set to default for**. • **Set to default for** - Sélectionnez un type de source de journal et cliquez sur la flèche gauche pour supprimer un type de source de journal de la liste **Set to default for**. Répétez cette étape pour chaque type de source de journal dont vous souhaitez substituer ou améliorer l'extension.

Etape 7 Cliquez sur **Browse** puis localisez un document d'extension de source de journal (`<filename>.xml`) si vous souhaitez télécharger un document d'extension pour remplacer le document d'extension existant.

Etape 8 Cliquez sur **Upload**.

Etape 9 Cliquez sur **Save**.

L'extension de source de journal est réexaminée. Le collecteur d'événement détecte automatiquement les changements et exécute l'extension de source de journal.

Copie d'une extension de source de journal

Cette section fournit des informations sur la manière de copier une extension de source de journal.

Utilisez cette fonction si vous souhaitez créer une nouvelle extension de source de journal comprenant certains ou tous les paramètres d'une extension de source de journal existante. Vous pouvez utiliser une extension de source de journal en tant que modèle.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Extensions**.

Etape 4 A partir de la liste d'extensions de source de journal, sélectionnez l'extension de source de journal que vous souhaitez copier

Etape 5 Cliquez que **Copy**.

Etape 6 Entrez les valeurs pour les paramètres :

Tableau 2-4 Copiez les paramètres d'extension de source de journal

Paramètre	Description
Nom	Entrez un nom pour l'extension de source de journal. Ce nom peut contenir un nombre maximal de 255 caractères alphanumériques plus le trait de soulignement (_).
Description	Entrez un nom pour l'extension de source de journal. La description ne peut pas être supérieure à 255 caractères.

Tableau 2-4 Copiez les paramètres d'extension de source de journal (suite)

Paramètre	Description
Conditions d'utilisation	Dans la zone de liste, sélectionnez l'une des options suivantes : • **Parsing Enhancement** - Sélectionnez cette option lorsque le gestionnaire de services de données analyse correctement la plupart des zones de la source de journal mais nécessite de corriger une ou deux zones. Ces valeurs de zone incorrectes sont améliorées avec les nouvelles valeurs XML. Il s'agit du paramètre par défaut. • **Parsing Override** - Sélectionnez cette option lorsque le gestionnaire de services de données ne parvient pas à analyser correctement les informations spécifiques et requises de l'unité, ou ne parvient pas à les extraire. Cette extension de source de journal redéfinit entièrement l'analyse défectueuse via le module de service de périphérique et substitue l'analyse avec les nouvelles valeurs XML.
Types de source de journal	Sélectionnez les sources de journal à ajouter ou supprimer de l'analyse d'extension. Les options comprennent : • **Available** - Sélectionnez un type de source de journal puis cliquez sur la flèche pour ajouter la source de journal à la liste **Set to default for**. • **Set to default for** - Sélectionnez un type de source de journal et cliquez sur la flèche gauche pour supprimer un type de source de journal de la liste **Set to default for**. Répétez cette étape pour chaque type de source de journal dont vous souhaitez substituer ou améliorer l'extension.

Etape 7 Cliquez sur **Save**.

La nouvelle extension de source de journal est créée. Le collecteur d'événement détecte automatiquement les changements et décroche une extension de source de journal nouvelle ou révisée.

Suppression d'une extension de source de journal

La suppression d'une extension de source de journal supprime toutes les améliorations ou substitutions d'analyse supplémentaires depuis la source de journal.

Si vous supprimez une extension de source de journal, les changements d'analyse sont immédiatement appliqués aux futurs événements pour les sources du journal influencées par le changement d'analyse.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Extensions**.

Etape 4 A partir de la liste d'extensions de source de journal, sélectionnez l'extension de source de journal que vous souhaitez supprimer

Etape 5 Cliquez sur **Delete**.

Etape 6 Cliquez sur **Yes** pour confirmer la suppression.

Activation ou désactivation d'une extension de source de journal

Vous pouvez activer ou désactiver une extension de source de journal dans QRadar, qui vous le permet.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources**.

Etape 3 Cliquez sur l'icône **Log Source Extensions**.

Etape 4 A partir de la liste d'extensions de source de journal, sélectionnez l'extension de source de journal que vous souhaitez activer ou désactiver.

Etape 5 Cliquez sur **Enable/Disable**.

Le statut (vrai ou faux) s'affiche dans la colonne Activée.

L'extension de source de journal est activée ou désactivée. Le collecteur d'événement détecte automatiquement les changements et exécute l'extension de source de journal.

A CRÉATION D'UN DOCUMENT D'EXTENSIONS

Les extensions de source de journal permettent de réparer un événement qui présente des informations manquantes incorrectes.

Vous pouvez également utiliser ces extensions pour analyser un événement lorsque le protocole DSM associé ne parvient pas à trouver un résultat. Tous les nouveaux événements créés par les extensions de source de journal sont associés au périphérique ayant échoué dans l'analyse des charges utiles d'origine. La création d'une extension empêche les événements inconnus ou non catégorisés d'être stockés comme inconnus QRadar.

Remarque : Ce document est destiné à ceux qui ont une connaissance approfondie des expressions régulières basées sur Java et du codage XML.

Pour en savoir plus sur la configuration des extensions de source de journal, voir **Gérer des extensions de source de journal**.

Avant de définir une extension de source de journal, vous devez générer un document d'extension.

Cette section fournit des informations sur ce qui suit :

- **A propos des documents d'extension**
- **Comprendre l'élément dans un document d'extension**
- **Créer un document d'extension**
- **ID de type de source de journal**

A propos des documents d'extension

Un document d'extension est indiqué en format Extensible Markup Language (XML) et peut être créé ou modifié à l'aide de n'importe quelle application de traitement de texte. Vous pouvez créer plusieurs documents d'extension et les associer à différents types de source de journal.

L'utilisation du format XML exige que toutes les expressions régulières soient contenues dans les sections de données de type caractère (CDATA) afin d'éviter

une interférence entre les caractères spéciaux et le format de balisage. Par exemple :

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[(tcp|udp|icmp|gre)]]></pattern>
```

Où `(tcp|udp|icmp|gre)` est le motif actuel d'expression régulière.

La configuration est constituée en deux sections : les motifs et les groupes de correspondance. Pour plus d'informations, voir **Comprendre l'élément dans un document d'extension**.

Comprendre l'élément dans un document d'extension

Cette section explique les types d'éléments qui composent un document d'extension dans QRadar.

Motifs

Plutôt que d'associer une expression régulière à un nom de zone particulier, les motifs (`patterns`) sont déclarés séparément dans la partie supérieure du document d'extension et peuvent ensuite être référencés dans le fichier à plusieurs reprises.

Remarque : Tous les caractères entre le <modèle> de balise ouvrante et le </modèle> de balise fermante sont considérés comme étant des composants du modèle. N'utilisez pas des espaces supplémentaires et des retours fixes ou autour de votre modèle ou expression <CDATA>. Les caractères ou espaces supplémentaires peuvent empêcher à l'extension DSM de trouver votre modèle prévu.

Tableau A-1 Paramètres de modèle

Paramètre	Description
`ID` (Obligatoire)	Entrez une chaîne régulière unique dans le document d'extension.
`insensible à la casse` (Facultatif)	Entrez un modèle pour ignorer la casse de caractère au moment d'établir une correspondance, par exemple `abc` est la même chose que `ABC`. Sinon, ce paramètre par défaut devient faux.
`trim-whitespace` (Facultatif)	Entrez cette fonction si vous souhaitez que le modèle ignore l'espace blanc et les retours chariot. Si les sections CDATA sont répartis en différentes lignes, ce paramètre montre que tous les espaces supplémentaires ainsi que les retours chariot ne sont pas interprétés comme faisant partie du modèle. Sinon, ce paramètre par défaut devient faux.

Groupes de correspondance

Un groupe de correspondance (`match-group`) est un ensemble de motifs utilisés pour l'analyse ou la modification d'un ou de plusieurs types d'événements. Un matcher est une entité présente dans un groupe de correspondance qui est

analysée (par exemple, EventName) et associée au motif ou groupe approprié pour l'analyse. Tout numéro des groupes de correspondance peuvent apparaître dans le document d'extension.

Tableau A-2 Match Group Parameters

Paramètre	Description
`order` (Obligatoire)	Entrez une valeur entière supérieure à zéro pour définir l'ordre dans lequel les groupes de correspondance doivent être exécutés. Elle doit être unique dans le document d'extension.
`description` (Facultatif)	Entrez une description pour le groupe de correspondance, qui peut être n'importe quelle chaîne. Ces informations peuvent apparaître dans les journaux d'événement. Sinon, ce paramètre par défaut devient vide.
`device-type-id-override` (Facultatif)	Définissez un ID d'unité différent afin de substituer QID. Permet au groupe de correspondance de rechercher le type d'événement dans le périphérique indiqué. Il doit être un ID type source de journal valide, représenté comme un entier. Une liste d'ID type source de journal est représentée dans **Tableau A-6**. Si cela n'est pas indiqué, ce paramètre devient par défaut le type source de journal auquel l'extension est attachée.

Les groupes de correspondance peuvent avoir jusqu'à trois différents types d'entités :

- **Matcher (matcher)**
- **Single-event modifier (event-match-single)**
- **Modificateur Multi-event (event-match-multiple)**

Matcher (`matcher`)

Une entité matcher est une zone analysée (par exemple, EventName) et associée au motif et groupe approprié pour l'analyse. Les matchers ont un ordre associé, ainsi au cas où plusieurs matchers sont indiqués pour le même nom de zone, les matchers sont traités selon l'ordre indiqué jusqu'à ce qu'une analyse réussie soit trouvée ou qu'un échec se produise.

Tableau A-3 Paramètres Matcher Entity

Paramètre	Description
Zone (Obligatoire)	Entrez la zone dans laquelle vous souhaitez appliquer le motif, par exemple EventName ou SourceIp. Voir **Tableau A-4** pour obtenir la liste des noms de zones valides.
ID de motif (Obligatoire)	Entrez le motif que vous souhaitez utiliser lors de l'analyse de la zone hors de la charge utile. Cette valeur doit correspondre (y compris la case) au paramètre ID du motif préalablement défini dans un paramètre ID du motif (**Tableau A-1**).

Tableau A-3 Paramètres Matcher Entity (suite)

Paramètre	Description
order (Obligatoire)	Entrez la commande que le motif doit essayer parmi les correspondances attribuées à la même zone. Si deux correspondances sont attribuées à la zone EventName, celle qui a la plus faible commande est attribuée en premier.
capture-group (Facultatif)	Définissez un groupe de capture, comme indiqué dans l'expression régulière entre les parenthèses ( ). Ces captures sont indexées par ordre croissant et sont traitées de la gauche à la droite dans le motif. La zone **capture-group** doit être un nombre entier positif inférieur ou égal au nombre de groupes de capture contenus dans le motif. La valeur par défaut est zéro, ce qui représente la correspondance complète. Par exemple, vous pouvez définir un motif unique pour une adresse IP source et un port ; où la correspondance SourceIp peut utiliser un groupe de capture de niveau 1 et la correspondance SourcePort un groupe de capture de niveau 2. Toutefois, un seul motif doit être défini. Cette zone a un double objectif lorsqu'elle est associée au paramètre **enable-substitutions**.

Tableau A-3 Paramètres Matcher Entity (suite)

Paramètre	Description
`enable-substitutions` (Facultatif)	Entrez ce paramètre booléen comme **`true`** lorsque la zone ne peut être représentée de manière adéquate avec une capture de groupe aussi droite que possible. Vous permet de combiner plusieurs groupes en même temps avec un texte supplémentaire pour former une valeur. Ce paramètre change la signification du paramètre **`capture-group`**. Le paramètre **`capture-group`** créé la nouvelle valeur, et des substitutions de groupe sont indiqués à l'aide **`\x`** where **`x`** is a group number from 1 to 9. Vous pouvez utiliser des groupes à plusieurs reprises et tous les textes à format libre peuvent également être insérés dans la valeur. Par exemple, si vous devez former une valeur du groupe 1, suivi d'un trait de soulignement, du groupe 2, d'un @, puis du groupe 1 à nouveau, la syntaxe appropriée du groupe de capture est : **`capture-group="\1_\2@\1"`** Dans un autre exemple, une adresse MAC est séparée par deux points, mais QRadar suppose que les adresses MAC sont séparées par un trait d'union. La syntaxe pour analyser et capturer des portions individuelles est : **`capture-group="\1:\2:\3:\4:\5:\6"`** Si aucun groupe n'est indiqué dans le groupe de capture lorsque les substitutions sont activées, un remplacement de texte direct se produit. La valeur par défaut est false.
`ext-data` (Facultatif)	Entrez un paramètre de données supplémentaires pour définir toutes les informations de zone supplémentaires ou le formatage qu'une zone de correspondance peut offrir dans l'extension. Par exemple, il est possible que vous disposiez d'un périphérique qui envoie des événements en utilisant un horodatage unique et vous souhaitiez que l'événement soit redéfini à l'heure du périphérique standard. Le paramètre ext-data inclus dans la zone DeviceTime vous permet de redéfinir la date et l'horodatage des événements. Pour plus d'informations, voir **Tableau A-4**.

Tableau A-4 fournit une liste de noms de zone valides à utiliser dans le paramètre de zone de matcher (voir **Tableau A-2**).

Tableau A-4 Noms de zone Matcher

Nom de zone	Description
EventName (Obligatoire)	Entrez le nom de l'événement à extraire du QID pour identifier l'événement.
Catégorie d'événement	Entrez une catégorie d'événement pour tout événement disposant d'une catégorie non gérée par une entité **`event-match-single`** ou **`event-match-multiple`**. Associée à EventName, la zone EventCategory est utilisée pour rechercher un événement dans QID.
SourceIp	Entrez l'adresse IP source du message.
SourcePort	Entrez le port source du message.
SourceIpPreNAT	Entrez l'adresse IP source du message avant que Network Address Translation (NAT) ne s'affiche.
SourceIpPostNAT	Entrez l'adresse IP source du message avant que NAT ne s'affiche.
SourceMAC	Entrez l'adresse MAC source du message.
SourcePortPreNAT	Entrez le port source du message avant que NAT ne s'affiche.
SourcePortPostNAT	Entrez le port source du message après l'affichage de NAT.
DestinationIp	Entrez l'adresse IP de destination du message.
DestinationPort	Entrez le port de destination du message.
DestinationIpPreNAT	Entrez l'adresse IP de destination du message après l'affichage de NAT.
DestinationIpPostNAT	Entrez l'adresse IP de destination du message après l'affichage de NAT.
DestinationPortPreNAT	Entrez le port destination du message avant que NAT ne s'affiche.
DestinationPortPostNAT	Entrez le port de destination du message après l'affichage de NAT.
DestinationMAC	Entrez l'adresse MAC de destination du message.

Tableau A-4 Noms de zone Matcher (suite)

Nom de zone	Description
DeviceTime	Entrez l'heure et le format utilisés par le périphérique. Cette date et l'horodatage représentent l'heure à laquelle l'événement a été envoyé, selon le périphérique (il ne s'agit PAS de l'heure d'arrivée de l'événement). La zone DeviceTime prend en charge la possibilité d'utiliser une date et un horodatage personnalisés pour l'événement en appelant l'entité ext-data Matcher. La liste suivante contient des exemples de formats de date et d'horodatage pouvant être utilisés dans la zone DeviceTime : • ext-data="dd/MMM/YYYY:hh:mm:ss" • ext-data="MMM dd YYYY / hh:mm:ss" • ext-data="hh:mm:ss:dd/MMM/YYYY" Pour en savoir plus sur les valeurs possibles de formats de date et d'horodatage, voir http://download.oracle.com/javase/1.4.2/docs/api/java/text/SimpleDateFormat.html. ***Remarque :*** *DeviceTime est la seule zone d'événement qui utilise le paramètre facultatif ext-data.*
Protocol	Entrez le protocole associé à l'événement, par exemple, TCP, UDP ou ICMP. Si un protocole n'est pas correctement analysé à partir d'un message, les ports analysés ne peuvent apparaître dans QRadar (il n'affiche que les ports des protocoles basés sur un port).
UserName	Entrez le nom d'utilisateur associé à l'événement.
HostName	Entrez le nom d'hôte associé à l'événement. En général, cette zone est associée aux événements d'identité.
GroupName	Entrez le nom de groupe associé à l'événement. En général, cette zone est associée aux événements d'identité.
NetBIOSName	Entrez le nom NetBIOS associé à l'événement. En général, cette zone est associée aux événements d'identité.
ExtraIdentityData	Entrez toutes les données spécifiques à l'utilisateur associées à l'événement. En général, cette zone est associée aux événements d'identité.
SourceIpv6	Entrez l'adresse IP source IPv6 du message.
DestinationIpv6	Entrez l'dresse IP source IPv6 de destination du message.

Single-event modifier (`event-match-single`)

Modificateur Single-event (`event-match-single`) correspond exactement (et modifie ensuite) à un type d'événement, comme indiqué par le paramètre EventName. Cette entité permet une mutation d'événements à succès en

changeant la catégorie d'événement, la gravité, ou la méthode pour envoyer des événements d'identité.

Lorsque des événements correspondants à ce nom d'événement sont analysés, la catégorie d'unité, la gravité, ainsi que les propriétés d'identité sont imposés sur les événements résultants. Une entité event-match-single comprend trois propriétés facultatives :

Tableau A-5 Single-Event Modifier Parameters

Paramètre	Description
device-event-category	Entrez une nouvelle catégorie pour rechercher l'événement dans QID. Il s'agit d'un paramètre d'optimisation, étant donné que certains périphériques ont la même catégorie pour tous les événements.
severity	Entrez la gravité de l'événement. Ce paramètre doit être une valeur entière comprise entre 1 et 10. Si une gravité de niveau inférieur à 1 ou supérieur à 10 est indiquée, le système utilise par défaut le niveau 5. Si rien n'est indiqué, la valeur par défaut est toute valeur trouvée dans QID.
send-identity	Indique l'envoi d'informations concernant le changement d'identité de l'événement. Sélectionnez l'une des options suivantes : • **UseDSMResults** – Si DSM retourne un événement d'identité, l'événement est transmis. Par contre si l'événement n'est pas renvoyée par DSM, celui-ci ne créé pas ou ne modifie pas les informations d'identité. Il s'agit de la valeur par défaut si aucune valeur n'est indiquée. • **SendIfAbsent** – Si DSM crée des informations d'identité, l'événement d'identité est transmis sans être affecté. Si aucun événement d'identité n'est créé par DSM, alors que les informations sont suffisantes pour le faire, un événement est généré avec toutes les zones définies. • **OverrideAndAlwaysSend** – Ignore les événements d'identité retournés par DSM et crée un nouvel événement si les informations sont suffisantes. • **OverrideAndNeverSend** – Supprimez les informations d'identité retournées par DSM.

Modificateur Multi-event (**event-match-multiple**)

Le modificateur d'événement multiples (**event-match-multiple**) correspond à une gamme de types d'événements (et modifie ensuite) comme indiqué par le paramètre **pattern-id** et le paramètre **capture-group-index**.

Remarque : Cette correspondance n'est pas effectuées contre la charge utile, mais plutôt contre les résultats du EventName précédemment analysée hors de la charge utile.

Cette entité permet une mutation d'événements à succès en changeant la catégorie d'événement, la gravité, ou la méthode pour envoyer des événements d'identité. La section **`capture-group-index`** doit être une valeur entière (les substitutions ne sont pas prise en charge) et l'ID du motif doit faire référence à une entité de motif existante. Toutes les autres propriétés sont identiques à leurs équivalents dans le modificateur d'événement unique

Créer un document d'extension

Cette section fournit des informations sur ce qui suit :

- **Ecriture d'un document d'extension complet**
- **Téléchargement de documents d'extension**
- **Résoudre des problèmes d'analyse spécifiques**

Ecriture d'un document d'extension complet

L'exemple du document d'extension inclus dans cette section fournit des informations sur la manière d'analyser un type particulier de Cisco FWSM de sorte que les événements ne soient pas envoyés avec un nom d'événement incorrect. Par exemple, si vous souhaitez résoudre le mot **`session`**, qui est intégré au milieu du nom de l'événement :

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015: Built UDP
connection for faddr 38.116.157.195/80 gaddr
129.15.127.254/31696 laddr 10.194.2.196/2157 duration 0:00:00
bytes 57498 (TCP FINs)
```

Cette condition ne permet pas au DSM de reconnaître tous les événements et ces derniers sont tous non analysés et associés à l'enregistreur générique.

Bien qu'une seule partie de la chaîne de texte (**`302015`**) soit utilisée pour la recherche QID, la chaîne de texte entière (**`%FWSM-session-0-302015`**) identifie l'événement comme provenant de Cisco FWSM. Puisque la chaîne de texte n'est pas valide, le DSM suppose que l'événement n'est pas valide.

Un périphérique FWSM dispose d'un grand nombre de types d'événements, plusieurs d'entre eux avec des formats uniques. L'exemple de document d'extension suivant montre comment analyser un type d'événement.

Remarque : Les ID de motif n'ont pas besoin de correspondre aux noms de zone qu'ils analysent. Même si l'exemple suivant duplique le motif, les zones SourceIp et SourceIpPreNAT peuvent utiliser le même motif dans ce cas (cela peut ne pas être valable avec les événements FWSM).

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
```

```
<pattern id="EventNameFWSM"
xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp" xmlns=""><![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT" xmlns=""><![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT" xmlns=""><![CDATA[laddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp" xmlns=""><![CDATA[faddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol" case-insensitive="true"
xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6" case-insensitive="true"
xmlns=""><![CDATA[ protocol=6]]></pattern>
<pattern id="EventNameId"
xmlns=""><![CDATA[(\d{1,6})]]></pattern>

<match-group order="1" description="FWSM Test"
device-type-id-override="6" xmlns="">
 <matcher field="EventName" order="1"
pattern-id="EventNameFWSM" capture-group="1"/>
 <matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="1" />
 <matcher field="SourcePort" order="1" pattern-id="SourceIp"
capture-group="2" />
 <matcher field="SourceIpPreNAT" order="1"
pattern-id="SourceIpPreNAT" capture-group="1" />
 <matcher field="SourceIpPostNAT" order="1"
pattern-id="SourceIpPostNAT" capture-group="1" />
 <matcher field="SourcePortPreNAT" order="1"
pattern-id="SourceIpPreNAT" capture-group="2" />
 <matcher field="SourcePortPostNAT" order="1"
pattern-id="SourceIpPostNAT" capture-group="2" />
 <matcher field="DestinationIp" order="1"
pattern-id="DestinationIp" capture-group="1" />
 <matcher field="DestinationPort" order="1"
pattern-id="DestinationIp" capture-group="2" />
 <matcher field="Protocol" order="1" pattern-id="Protocol"
capture-group="1" />
 <matcher field="Protocol" order="2" pattern-id="Protocol_6"
capture-group="TCP" enable-substitutions=”true”/>

 <event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Cisco
Firewall"/>
</match-group>

</device-extension>
```

L'exemple du document d'extension ci-dessus démontre quelques-uns des aspects fondamentaux d'analyse :

- Adresses IP
- Ports
- Protocole
- Plusieurs zones utilisant le même motif avec différents groupes

Cet exemple analyse tous les événements FWSM qui suivent le motif indiqué, bien que les zones analysées puissent ne pas être présentes dans ces événements (si les événements comportent un contenu différent).

Les informations nécessaires à la création de cette configuration indisponibles à partir de l'événement :

- Le nom de l'événement est représenté par les six derniers chiffres (`302015`) de la `%FWSM-session-0-302015` portion d'événement.
- FWSM possède une catégorie log source type codée en dur de `Cisco Firewall`.
- FWSM utilise le QID Cisco Pix et inclut par conséquent le paramètre `device-type-id-override="6"` dans le groupe de correspondance (l'ID de type source de journal de pare-feu Pix est 6, voir **Tableau A-6**).

Remarque : Si les informations QID ne sont pas indiquées ou ne sont pas disponibles, vous pouvez modifier le mappage de l'événement. Pour plus d'informations, voir la section Modification du mappage de l'événement dans *IBM Security QRadar - Guide d'utilisation.*

Un nom d'événement et une catégorie d'événement du périphérique sont requis au moment de rechercher un événement dans le QID. Cette catégorie d'événement de périphérique est un paramètre de groupement à l'intérieur de la base de données qui permet de définir des événements d'un périphérique. La fonction `event-match-multiple` située à l'extrémité du groupe de correspondance comprend un codage en dur de la catégorie. La fonction `event-match-multiple` utilise le motif EventNameId sur le nom d'événement analysé pour faire correspondre un maximum de six chiffres. Ce motif n'est pas exécuté contre la charge utile, la portion est analysée en tant que zone EventName.

Le motif EventName fait référence à la portion `%FWSM` des événements ; tous les événements FWSM Cisco contiennent la portion `%FWSM`. Le motif dans l'exemple correspond à `%FWSM` suivi d'un nombre quelconque (zéro ou plus) de lettres et de traits. Ce motif résout le mot `session` qui est intégré au milieu du nom d'événement à supprimer. La gravité d'événement (selon Cisco), suivi d'un trait puis du nom d'événement réel comme prévu par QRadar. La seule chaîne avec un groupe de capture (délimitée par des parenthèses) est ce motif de chiffre `(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`.

Les adresses IP et les ports d'événement suivent tous le même motif de base : une adresse IP suivie d'une barre oblique puis du numéro de port numérique. Ce motif analyse deux éléments de données (l'adresse IP et le port) et indique les différents groupes de capture de la section de correspondance.

```
   <matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourceIp"
capture-group="2" />
```

Ainsi, les motifs d'adresse IP/port représentent quatre ensembles de un à trois chiffres, séparés par des périodes suivies par une barre oblique et par le numéro de port. La section IP address est dans un groupe, comme le numéro de port (sauf la barre oblique). Comme mentionné précédemment, les sections de correspondance pour ces zones font référence au même nom de motif, mais à un groupe de capture différent (l'adresse IP correspond au groupe 1 et le port au groupe 2).

Le protocole est un motif commun qui recherche la charge utile pour la première instance de protocole TCP, UDP, ICMP ou GRE (le motif est marqué avec le paramètre insensible à la casse de sorte que toutes les occurrences correspondent).

Remarque : Vous devez rechercher le protocole au moment de créer des documents d'extension, étant donné que QRadar peut ne pas afficher les numéros de port si l'événement n'est pas basé sur un protocole de port. Voir la section **Convertir un protocole** pour obtenir un exemple sur la façon de rechercher un protocole.

Bien qu'un second motif de protocole ne se produise pas dans l'événement qui est en cours d'utilisation en tant qu'exemple, il existe un autre défini en seconde position. Si le dernier motif de protocole ne correspond pas, essayez l'autre (et ainsi de suite). Le second motif de protocole démontre également une substitution directe ; il n'existe aucun groupe de correspondance dans le motif, mais avec le paramètre de substitutions activé, le texte TCP peut être utilisé à la place du protocole=6.

Téléchargement de documents d'extension

Plusieurs documents d'extension peuvent être créés, téléchargés et associés à différents types de source de journal. Les documents d'extension peuvent être stockés n'importe où avant de télécharger QRadar. Lorsque vous sélectionnez un document d'extension pour le téléchargement, QRadar valide le document contre le XSD interne. QRadar vérifie également la validité du document avant de télécharger le système.

Résoudre des problèmes d'analyse spécifiques

Cette section vous fournit des exemples XML pouvant être utilisés pour résoudre des problèmes spécifiques d'analyse.

- **Convertir un protocole**
- **Exécuter une substitution unique**

- **Génération d'une adresse MAC séparée par deux points**
- **Combinaison de l'adresse IP et du port**
- **Modification d'une catégorie d'événement**
- **Modification de plusieurs catégories d'événements**
- **Suppression d'événements de changement d'identité**
- **Codage des journaux**

Convertir un protocole

l'exemple suivant illustre une conversion de protocole typique qui recherche les protocoles TCP, UDP, ICMP ou GRE dans la charge utile, entourés par une limite de mot (par exemple, onglet, espace, fin de ligne). En outre, la case des caractères est ignorée :

```
<pattern id="Protocol" case-insensitive="true"
xmlns=""><![CDATA[\b(tcp|udp|icmp|gre)\b]]> </pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol"
capture-group="1" />
```

Exécuter une substitution unique

L'exemple suivant est une substitution linéaire qui analyse l'adresse IP source, puis remplace le résultat et définit l'adresse IP en 10.100.100.100, en l'ignorant dans la charge utile. Cet exemple suppose que l'adresse IP correspond à quelque chose de similaire à SrcAddress=10.3.111.33 suivi d'une virgule :

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]]></p
attern>

<matcher field="SourceIp" order="1"
pattern-id="SourceIp_AuthenOK" capture-group="100.100.100.100"
enable-substitutions="true"/>
```

Génération d'une adresse MAC séparée par deux points

QRadar détecte des adresses MAC sous une forme séparée par deux points. Etant donné que tous les périphériques n'utilisent pas ce formulaire, l'exemple suivant montre comment résoudre ce problème :

```
<pattern id="SourceMACWithDashes"
xmlns=""><![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-(
[0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{
2})]]></pattern>

<matcher field="SourceMAC" order="1" pattern-id="
SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```

Dans l'exemple ci-dessus, `SourceMAC=12-34-56-78-90-AB` est converti en adresse MAC de `12:34:56:78:90:AB`.

Si les tirets sont retirés du motif, celui-ci convertit l'adresse MAC sans séparateurs. Si des espaces sont insérés, le motif convertit l'adresse MAC séparée par des espaces, etc.

Combinaison de l'adresse IP et du port

En général une adresse IP et un port sont combinés dans une zone, séparés par deux points ou une barre oblique. L'exemple suivant utilise plusieurs groupes de capture avec un motif :

```
pattern id="SourceIPColonPort" xmlns=""><!
[CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]
]></pattern>

<matcher field="SourceIp" order="1"
pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1"
pattern-id="SourceIPColonPort" capture-group="2" />
```

Modification d'une catégorie d'événement

Une catégorie d'événement du périphérique peut être codée en dur, ou la gravité doit être ajustée. L'exemple suivant permet d'ajuster la gravité d'un type d'événement unique :

```
<event-match-single event-name="TheEvent"
device-event-category="Actual Category" severity="6"
send-identity="UseDSMResults" />
```

Modification de plusieurs catégories d'événements

L'exemple suivant est similaire à l'exemple d'événement unique ci-dessus, sauf que cet exemple correspond à tous les codes d'événement commençant par `7` et suivi d'un à cinq chiffres :

```
<pattern id="EventNameId"
xmlns=""><![CDATA[(7\d{1,5})]]></pattern>

<event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Actual Category"
severity="6" send-identity="UseDSMResults"/>
```

Suppression d'événements de changement d'identité

Un DSM peut inutilement envoyer des événements de changement d'identité. Voici deux exemples ; l'un porte sur la méthode de suppression des événements de changement d'identité devant être envoyés à partir d'un type d'événement unique. L'autre porte sur la méthode de suppression des événements de changement d'identité devant être envoyés à partir d'un groupe d'événements.

```
// N'envoyez jamais l'identité de l'événement avec un nom
d'événement "Authen OK"
<event-match-single event-name="Authen OK"
```

```
device-event-category="ACS" severity="6"
send-identity="OverrideAndNeverSend" />

// N'envoyez jamais une identité d'un événement ayant un nom
d'événement commençant par 7, suivi de un à cinq chiffres :
<pattern id="EventNameId"
xmlns=""><![CDATA[(7\d{1,5})]]></pattern>

<event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Cisco Firewall"
severity="7" send-identity="OverrideAndNeverSend"/>
```

Codage des journaux

Les formats de codage suivants sont pris en charge :

- US-ASCII
- UTF-8

Les journaux peuvent être transmis au système dans un codage qui ne correspond pas aux formats de type US-ASCII or UTF-8. Vous pouvez configurer un indicateur avancé pour vous assurer que l'entrée peut être codée à nouveau au format UTF-8 pour des fins d'analyse et de stockage.

Par exemple, si vous voulez être sûr que les journaux sources arrivent en format de codage SHIFT-JIS (ANSI/OEM Japanese), procédez comme suit :

```
<device-extension source-encoding=″SHIFT-JIS″
xmlns=″event_parsing/device_extension″>
```

Les journaux sont insérés au format UTF-8.

Formatage des dates d'événement et des horodatages

Une extension de source de journal pourQRadar peut détecter plusieurs formats de date et d'horodatage sur les événements. Etant donné que les fabricants de périphérique ne sont pas conforme à une norme de format de date et d'horodatage, le paramètre facultatif ext-data est compris dans l'extension source de journal afin que DeviceTime soit redéfini. L'exemple suivant montre comment redéfinir un événement afin de corriger le formatage de date et d'horodatage :

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern
id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]
</pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
<matcher field="EventName" order="1" pattern-id="EventName1"
capture-group="1"/>
<matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
<matcher field="UserName" order="1" pattern-id="Username"
capture-group="1"/></match-group>
```

ID de type de source de journal

Tableau A-6 répertorie les ID de type de source pouvant être utilisés dans une instruction `match-group` :

Tableau A-6 Numéros d'ID de type source de journal

ID	Type source de journal
2	Snort Open Source IDS
3	Pare-feu-1 Check Point
4	Filtre de pare-feu configurable
5	Pare-feu réseau et VPN Juniper
6	Pare-feu PIX Cisco
7	Filtre de messages d'authentification configurable
9	Enterasys Dragon Network IPS
10	Apache HTTP Server
11	Système d'exploitation Linux
12	Journal d'événements de sécurité Microsoft Windows
13	Logiciel IIS de Windows
14	Pare-feu iptables de Linux
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Détection et prévention d'intrusion des réseaux Juniper (IDP)
19	Système de prévention d'intrusions (IPS) TippingPoint
20	Cisco IOS
21	Commutateur VPN Nortel Contivity
22	Routeur Multiprotocoles Nortel
23	Cisco VPN 3000 Series Cntrator
24	Messages d'authentification du système d'exploitation Solaris
25	Dispositif McAfee IntruShield Network IPS
26	Cisco CSA
28	Commutateur Enterasys Matrix E1
29	Journaux Sendmail du système d'exploitation Solaris
30	Système de prévention d'intrusions Cisco (IDS)
31	Firewall Services Module (FWSM) Cisco
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS Family
36	Juniper Networks Secure Access (SA) SSL VPN
37	Commutateur VPN Nortel Contivity
38	Système de prévention d'intrusions (IPS) Top Layer
39	Universal DSM

Tableau A-6 Numéros d'ID de type source de journal (suite)

ID	Type source de journal
40	Tripwire Enterprise
41	Dispositif Cisco Adaptive Security (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web Proxy
47	Système de prévention d'intrusions (IPS) Ambiron TrustWave ipAngel
48	Oracle RDBMS Audit Records
49	F5 Networks BIG-IP LTM
50	Journaux du protocole DHCP du système d'exploitation Solaris
55	Array Networks SSL VPN Access Gateway
56	Cisco CatOS for Catalyst Switches
57	Serveur ProFTPD
58	Serveur DHCP Linux
59	Contrôleur Infranet des réseaux Juniper
64	Plateforme Juniper JunOS
68	Commutateur Enterasys Matrix K/N/S
70	Système d'exploitation Extreme Networks ExtremeWare
71	Dispositif Sidewinder G2 Security
73	Passerelle de sécurité Fortinet FortiGate
78	Périphérique SonicWall UTM/Firewall/VPN
79	Vericept Content 360
82	Dispositif Symantec Gateway Security (SGS)
83	Juniper Steel Belted Radius
85	Serveur AIX IBM
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	Dispositif CiscoNAC
96	Dispositifs TippingPoint série X
97	Microsoft DHCP Server
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend Interscan VirusWall

Tableau A-6 Numéros d'ID de type source de journal (suite)

ID	Type source de journal
101	Microsoft SQL Server
102	MAC OS X
103	Dispositif Bluecoat SG
104	Nortel Switched Firewall 6000
106	Commutateur 3Com 8800
107	Passerelle VPN Nortel
108	Détecteur d'intrusions Threat Protection System (TPS) Nortel
110	Commutateur Nortel Application
111	Plateforme Juniper DX Application Acceleration
112	SNARE Reflector Server
113	Routeurs Cisco série 12000
114	Commutateurs Cisco série 6500
115	Routeurs Cisco série 7600
116	Cisco Carrier Routing System
117	Routeur Cisco Integrated Services
118	Juniper M-Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Routeur Juniper MX-Series Ethernet Services
123	Plateforme Juniper T-Series Core
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	Système d'exploitation OpenBSD
139	Commutateur Juniper Ex-Series Ethernet
140	Sysmark Power Broker
141	Programme d'écoute de base de données Oracle
142	Samhain HIDS
143	Contrôleur de service Bridgewater Systems AAA
144	Paire de valeurs de nom
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron
150	Passerelle de services Juniper SRX
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere

Tableau A-6 Numéros d'ID de type source de journal (suite)

ID	Type source de journal
155	Contrôleur Aruba Mobility
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Routeurs Enterasys XSR Security
167	Commutateurs Enterasys Stackable et Standalone
168	Juniper Networks AVT
169	OS Services Qidmap
170	Enterasys A-Series
171	Enterasys B2-Series
172	Enterasys B3-Series
173	Enterasys C2-Series
174	Enterasys C3-Series
175	Enterasys D-Series
176	Enterasys G-Series
177	Enterasys I-Series
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro
194	Pare-feu ACE Cisco

Tableau A-6 Numéros d'ID de type source de journal (suite)

ID	Type source de journal
195	IBM DB2
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Oracle RDBMS OS Audit Record
206	Palo Alto PA Series
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	Serveur d'application IBM WebSphere
213	F5 Networks BIG-IP ASM
214	FireEye
215	Avertissement juste
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	Passerelle Web McAfee
221	CA Access Control Facility (ACF2)
222	Application McAfee / contrôle des changements
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron Smart Meter
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Dispositif de sécurité Web Sophos
241	Passerelle de sécurité Sophos Astaro
243	Infoblox NIOS

Tableau A-6 Numéros d'ID de type source de journal (suite)

ID	Type source de journal
244	Tropos Control
245	Novell eDirectory
249	IBM Guardium
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Commutateur Digital China Networks séries DCS et DCRS
264	Collecteur de journal Juniper Security Binary
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Hauwei S Series Switch
271	HBGary Active Defense
272	APC UPS
272	Cisco Wireless LAN Controller
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
282	OSSEC
283	Routeur Huawei AR Series
286	IBM AIX Audit
287	Serveur universel Symantec PGP
289	IBM Tivoli Endpoint Manager
290	Sécurité Web Juniper Mykonos
291	Nominum Vantio
292	Commutateur Enterasys 800-Series
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager

Tableau A-6 Numéros d'ID de type source de journal (suite)

ID	Type source de journal
296	F5 Networks BIG-IP Advanced Firewall Manager (AFM)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
304	IBM Security Access Manager for Enterprise Single Sign-on
309	ObserveIT

B INSTALLATION DE SOURCES DE PROTOCOLE

QRadar est préconfiguré pour effectuer automatiquement des mises à jour hebdomadaires pour les DSM, les protocoles et le module de scanner.

Si aucune mise à jour ne s'affiche dans la fenêtre des mises à jour, soit votre système n'a pas été assez longtemps opérationnel pour récupérer les mises à jour hebdomadaires, soit les mises à jour n'ont pas été effectuées. Si cela se produit, vous pouvez manuellement vérifier les nouvelles mises à jour. Pour plus d'informations sur la planification des mises à jour en attente, voir *IBM Security QRadar Administration Guide*.

Planification automatique des mises à jour

QRadar effectue des mises à jour automatiques sur une planification récurrente en fonction des paramètres de la page de configuration de mise à jour ; toutefois, si vous souhaitez planifier l'exécution d'une ou de plusieurs mises à jour à une heure spécifique, vous pouvez planifier une mise à jour en utilisant la fenêtre Planifier les mises à jour.

La mise à jour automatique est importante lorsque vous souhaitez planifier l'exécution d'une grande mise à jour durant les heures creuses, ainsi via la réduction de tous les impacts de performance sur votre système. Vous pouvez télécharger et installer automatiquement des mises à jour en utilisant l'icône Auto Updates sur l'onglet **Admin** ou installer manuellement une mise à jour de protocole.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **System Configuration**.

Etape 3 Cliquez sur l'icône **Auto Update**.

Etape 4 Facultatif. Si vous souhaitez planifier des mises à jour spécifiques, sélectionnez les mises à jour que vous souhaitez planifier.

Etape 5 Dans la zone de liste **Schedule**, sélectionnez le type de mise à jour que vous souhaitez planifier. Les options comprennent :

- All Updates
- Selected Updates

- Mises à jour de gestionnaire de service de données, scanner et protocole
- Mises à jour mineures

La fenêtre Schedule the Updates s'affiche.

Remarque : Les mises à jour du protocole installées automatiquement vous exigent de redémarrer Tomcat manuellement. Pour plus d'informations sur le redémarrage manuel de Tomcat, voir **Installation manuelle d'un protocole de source de journal**.

Etape 6 En utilisant l'agenda, sélectionnez la date et l'heure de début au moment où vous souhaitez démarrer vos mises à jour planifiées.

Etape 7 Cliquez sur **OK**.

Les mises à jour sélectionnées sont maintenant planifiées.

Affichage de mises à jour en attente

Si vous rencontrez des problèmes de connexion à un protocole, vous devez installer une mise à jour de protocole.

Toutes les mises à jour logicielles en attente deQRadar sont disponibles dans l'onglet **Admin**. Vous pouvez sélectionner et installer une mise à jour en attente depuis la fenêtre Auto Update.

Procédure

Etape 1 Cliquez sur l'onglet **Admin**.

Etape 2 Dans le menu de navigation, cliquez sur **System Configuration**.

Etape 3 Cliquez sur l'icône **Auto Update**.

La fenêtre Updates s'affiche. La fenêtre affiche automatiquement la page Check for Updates, en fournissant les informations suivantes :

Tableau B-1 Vérifiez les paramètres de la fenêtre des mises à jour

Paramètre	Description
Les mises à jour ont été installées	Indique que la dernière mise à jour de la date et de l'heure a été installée.
La prochaine mise à jour a été planifiée	Indique que la dernière mise à jour de la date et de l'heure est prévue pour l'installation. S'il n'existe aucune date ou heure indiquée, la mise à jour ne sera pas prévue pour l'exécution.
Nom	Indique le nom de la mise à jour.
Type	Indique le type de mise à jour. Les types comprennent : • Mises à jour de gestionnaire de service de données, scanner et protocole • Mises à jour mineures

Tableau B-1 Vérifiez les paramètres de la fenêtre des mises à jour (suite)

Paramètre	Description
Statut	Indique le statut de la mise à jour. Les types de statut comprennent : • **Nouvelle** - La mise à jour n'est pas encore prévue pour l'installation. • **Planifiée** - La mise à jour n'est pas prévue pour l'installation. • **Installation** - La mise à jour est en cours d'installation. • **Echec** - L'installation de la mise à jour a échoué.
Date d'installation	Indique que la dernière mise à jour de la date et de l'heure est prévue pour l'installation.

La barre d'outils de la page Check for Updates fournit les fonctions suivantes :

Tableau B-2 Fonctions de la barre d'outils des paramètres de la page Check for Updates

Fonction	Description
Masquer	Sélectionnez une ou plusieurs mises à jour puis cliquez sur **Hide** pour supprimer les mises à jour sélectionnées depuis la page Check for Updates. Vous pouvez afficher ou restaurer les mises à jour masquées sur la page Restore Hidden Updates. Pour plus d'informations, voir *IBM Security QRadar Administrator Guide*.
Installer	Dans la zone de liste, vous pouvez installer manuellement les mises à jour. Lorsque vous installez manuellement les mises à jour, le processus d'installation démarre en une minute. Pour plus d'informations, voir *IBM Security QRadar Administrator Guide*.
Planification	Dans cette zone de liste, vous pouvez configurer la date et l'heure spécifiques pour installer manuellement les mises à jour sélectionnées sur votre Console. Ceci est important lorsque vous souhaitez planifier l'installation de la mise à jour durant les heures creuses. Pour plus d'informations, voir *IBM Security QRadar Administrator Guide*.
Déprogrammer	Dans cette zone de liste, vous pouvez supprimer les planifications préconfigurées pour les mises d'installation manuelle sur votre Console. Pour plus d'informations, voir *IBM Security QRadar Administrator Guide*.
Rechercher par nom	Dans cette zone de texte, vous pouvez entrer un mot-clé et ensuite appuyer sur la touche Entrée pour localiser une mise à jour spécifique par nom.
Actualisation suivante	Ce compteur affiche la durée de la prochaine actualisation automatique. La liste des mises à jour sur la page de vérification des mises à jour s'actualise automatiquement toutes les 60 secondes. L'horloge est automatiquement mise en pause lorsque vous sélectionnez une ou plusieurs mises à jour.
Pause	Cliquez sur l'icône pour mettre le processus d'actualisation automatique en pause. Pour reprendre l'actualisation automatique, cliquez sur l'icône **Play**.

Tableau B-2 Fonctions de la barre d'outils des paramètres de la page Check for Updates

Fonction	Description
Actualiser	Cliquez sur l'icône pour actualiser manuellement la liste des mises à jour.

Etape 4 Pour afficher les détails d'une mise à jour, sélectionnez la mise à jour.

La description ainsi que tous les messages d'erreur s'affichent dans le panneau de la fenêtre.

Installation manuelle d'un protocole de source de journal

Vous pouvez installer une source de protocole qui vous permet d'accéder aux protocoles mis à jour ou supplémentaires pour l'utilisation de vos modules de support de périphérique et des sources de votre journal.

Installation d'un protocole individuel

Vous pouvez télécharger et installer manuellement les mises à jour lorsque QRadar n'inclut pas l'accès à Internet pour recevoir des mises à jour automatiques.

Procédure

Etape 1 Téléchargez le fichier du protocole à partir de l'un des sites Web suivants sur le système qui héberge QRadar.

http://www.ibm.com/support

Etape 2 En utilisant Secure Shell, connectez-vous à QRadar en tant que superutilisateur.

Nom d'utilisateur : **root**

Mot de passe : **<password>**

Etape 3 Naviguez jusqu'à l'annuaire comprenant le fichier téléchargé.

Etape 4 Entrez la commande suivante :

rpm -Uvh <filename>

L'emplacement **<filename>** est le nom du fichier téléchargé.

Par exemple : **rpm -Uvh PROTOCOL-SNMP-7.0-201509.noarch.rpm**

Pour compléter l'installation, vous devez exécuter un déploiement complet et redémarrer Tomcat.

Etape 5 Connectez-vous à QRadar.

https://**<IP Address>**

Où **<IP Address>** est l'adresse IP de votre QRadar.

Etape 6 Cliquez sur l'onglet **Admin**.

Etape 7 Sélectionnez **Advanced > Deploy Full Configuration**.

ATTENTION : *Le déploiement de la configuration complète redémarre plusieurs services sur le système QRadar. La collecte d'événements est indisponible sur QRadar jusqu'à ce que la configuration complète du déploiement soit terminée.*

Etape 8 En utilisant Secure Shell, connectez-vous à QRadar en tant que superutilisateur.

Nom d'utilisateur : **root**

Mot de passe : **<password>**

Etape 9 Redémarrer le service Tomcat :

redémarrage du service tomcat

Remarque : Le redémarrage de Tomcat sur QRadar force tout utilisateur à se connecter immédiatement. Vérifiez que tous les utilisateurs se sont déconnectés du système avant le redémarrage du service Tomcat.

Installation d'un ensemble de protocoles de source de journal

Le site Web de support IBM contient un ensemble de protocoles qui est mis à jour avec les dernières versions du protocole.

Procédure

Etape 1 Téléchargez l'ensemble de protocoles sur le système hébergeant QRadar.

http://www.ibm.com/support

Etape 2 En utilisant Secure Shell, connectez-vous à QRadar en tant que superutilisateur.

Nom d'utilisateur : **root**

Mot de passe : **<password>**

Etape 3 Naviguez jusqu'à l'annuaire comprenant le fichier téléchargé.

Etape 4 Entrez la commande suivante pour extraire l'ensemble du protocole :

tar -zxvf QRadar_bundled-PROTOCOL-<version>.tar.gz

où **<version>** est votre version de QRadar.

Etape 5 Entrez la commande suivante :

for FILE in *Common*.rpm PROTOCOL-*.rpm; do rpm -Uvh "$FILE"; done

Les protocoles sont installés. Pour compléter l'installation, vous devez exécuter un déploiement complet et redémarrer Tomcat.

Etape 6 Connectez-vous à QRadar.

https://**<IP Address>**

Où **<IP Address>** est l'adresse IP de votre QRadar.

Etape 7 Cliquez sur l'onglet **Admin**.

Etape 8 Sélectionnez **Advanced > Deploy Full Configuration**.

ATTENTION : *Le déploiement de la configuration complète redémarre plusieurs services sur QRadar. La collecte d'événements est indisponible sur QRadar jusqu'à ce que la configuration complète du déploiement soit terminée.*

Etape 9 En utilisant Secure Shell, connectez-vous à QRadar en tant que superutilisateur.

Nom d'utilisateur : **`root`**

Mot de passe : **`<password>`**

Etape 10 Redémarrer le service Tomcat :

```
redémarrage du service tomcat
```

Remarque : Le redémarrage de Tomcat sur QRadar force tout utilisateur à se connecter immédiatement. Vérifiez que tous les utilisateurs se sont déconnectés du système avant le redémarrage du service Tomcat.

C CONFIGURATION DU MODÈLE DCOM

Les protocoles Journal des événements de sécurité Microsoft et Personnalisation du journal des événements de sécurité Microsoft fournissent un ensemble de journaux d'événements Windows à distance et sans agent à l'aide de LAPI Microsoft Windows Management Instrumentation (WMI).

Pour configurer le modèle DCOM, sélectionnez le système d'exploitation à partir des options suivantes :

- Pour configurer les modèles DCOM et WMI de Windows Server 2003. Pour en savoir plus, voir **Configuration de Windows Server 2003**.
- Pour configurer les modèles DCOM et WMI de Windows Server 2008. Pour en savoir plus, voir **Configurez Windows Server 2008**.

Systèmes d'exploitation pris en charge

QRadar prend en charge l'interface de programme d'application Microsoft Windows Management Instrumentation (WMI) suivante :

- Microsoft Windows 2000
- Microsoft WIndows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R2
- Microsoft Windows XP
- Microsoft WIndows Vista
- Microsoft Windows 7

Avant de commencer

Avant d'installer le protocole du journal d'événements Windows, vous devez configurer les paramètres de votre système DCOM pour chaque hôte à contrôler. Assurez-vous que les éléments suivants sont configurés pour chaque hôte :

- Configurez puis activez le modèle DCOM sur l'ordinateur hôte.
- Activez Windows Management Instrumentation sur l'ordinateur hôte.
- Activez le service registre à distance.
- Assurez-vous de disposer des autorisations administratives ou utilisateurs appropriées pour les modèles DCOM et WMI. Pour ce processus, vous devez être membre du groupe Administrateurs ou créer un groupe avec les autorisations requises vous permettant d'accéder à l'ordinateur à distance. Si le

système fait partie d'un domaine, vous devez être membre du groupe Administrateurs de domaine.

- Assurez-vous de configurer les pare-feu permettant le transfert des données sur le port TCP 135, ainsi que les communications DCOM 1024 sur votre réseau.

Configuration de Windows Server 2003

Pour configurer le modèle DCOM sur Windows Server 2003, procédez comme suit :

1. Vérifiez que les services Windows Server 2003 requis sont lancés. Pour en savoir plus, voir **Services DCOM et WMI requis de Windows Server 2003**.
2. Activation du modèle DCOM de Windows Server 2003. Pour plus d'informations, voir **Activation de DCOM pour Windows Server 2003**.
3. Configurez les communications DCOM de Windows Server 2003. Pour en savoir plus, voir **Configuration des communications DCOM dans Windows Server 2003**.
4. Configurez les comptes utilisateurs du modèle DCOM. Pour en savoir plus, voir **Configurez les comptes utilisateur Windows Server 2003 pour DCOM**.
5. Configurez WMI de Windows Server 2003. Pour plus d'informations, voir **Configuration de l'accès utilisateur WMI pour Server 2003**.
6. Testez la configuration WMI. Pour en savoir plus, voir **Vérification des communications WMI**.

Services DCOM et WMI requis de Windows Server 2003

Les services Windows suivants du modèle DCOM doivent être lancés et configurés pour un démarrage automatique :

- Serveur
- Registre à distance
- Windows Management Instrumentation

Vous pouvez configurer le serveur et les services de registre à distance pour un démarrage automatique.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
services.msc
```

Etape 3 Cliquez sur **OK**.

Etape 4 Dans le panneau Details, vérifiez que les services suivants sont lancés et définis pour un démarrage automatique :

- Serveur
- Registre à distance

Etape 5 Pour modifier une propriété du service, cliquez avec le bouton droit de la souris sur le nom du service, puis cliquez sur **Properties**.

Etape 6 A l'aide de la zone de liste **Startup type**, sélectionnez **Automatic**.

Etape 7 Si le statut de service ne démarre pas, cliquez sur **Start**.

Etape 8 Cliquez sur **OK**.

Etape 9 Fermez la fenêtre Services.

Vous êtes désormais prêt à activer DCOM sur votre ordinateur Windows Server 2003.

Activation de DCOM pour Windows Server 2003

Pour activer DCOM sur votre système Windows Server 2003, procédez comme suit :

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
dcomcnfg
```

Etape 3 Cliquez sur **OK**.

La fenêtre Component Services s'affiche.

Etape 4 Dans la partie **Console root**, ouvrez **Component Services** et **Computers**, puis sélectionnez **My Computer**.

Etape 5 Dans le menu **Action**, cliquez sur **Properties**.

Etape 6 Sélectionnez l'onglet **Default Properties**.

Etape 7 Configurez les propriétés par défaut suivantes :

a Sélectionnez la case **Enable Distributed COM on this computer**.

b A l'aide de la zone de liste **Default Authentication Level**, sélectionnez **Connecter**.

c A l'aide de la zone de liste **Default Impersonation Level**, sélectionnez **Identifier**.

Remarque : Vous pouvez définir les ports TCP qu'utilise le modèle DCOM pour communiquer sur votre réseau en configurant les propriétés des protocoles TCP/IP orientés connexion. Pour en savoir plus, voir **Configuration des communications DCOM dans Windows Server 2003**.

Etape 8 Cliquez sur **Apply**, puis sur **OK**.

Etape 9 Fermez la fenêtre Component Services.

Vous pouvez désormais configurer les ports DCOM sur votre système Windows Server 2003.

Configuration des communications DCOM dans Windows Server 2003

Windows Server 2003 requiert un protocole TCP/IP pour communiquer avec le modèle DCOM.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
dcomcnfg
```

Etape 3 Cliquez sur **OK**.

La fenêtre Component Services s'affiche.

Etape 4 Dans la partie **Console root**, ouvrez **Component Services** et **Computers**, puis sélectionnez **My Computer**.

Etape 5 Dans le menu **Action**, cliquez sur **Properties**.

Etape 6 Sélectionnez l'onglet **Default protocols**.

Etape 7 Configurez les options suivantes :

a Si Connection-oriented TCP/IP est répertorié dans la fenêtre DCOM Protocols, accédez à **Etape 8**.

b Si Connection-oriented TCP/IP n'est pas répertorié dans la fenêtre DCOM Protocol, sélectionnez **Add**.

La fenêtre de protocole Select DCOM s'affiche.

c Dans la zone de liste, sélectionnez **Connection-oriented TC/IP**.

Etape 8 Cliquez sur **OK**.

Etape 9 Cliquez sur **OK**.

Etape 10 Fermez la fenêtre Component Services.

Vous pouvez maintenant configurer un compte utilisateur avec l'autorisation d'accéder à l'hôte. Pour en savoir plus, voir **Configurez les comptes utilisateur Windows Server 2003 pour DCOM**.

Configurez les comptes utilisateur Windows Server 2003 pour DCOM

Après avoir activé DCOM, vous devez attribuer au compte une autorisation d'accès à DCOM sur l'hôte.

Vous devez sélectionner un compte existant avec accès administrateur ou créer un compte utilisateur normal membre d'un groupe administrateur afin d'accéder à l'hôte.

Vous devez configurer un compte utilisateur DCOM sur votre système Windows Server 2003.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
dcomcnfg
```

Etape 3 Cliquez sur **OK**.

La fenêtre Component Services s'affiche.

Etape 4 Dans la partie **Console root**, ouvrez **Component Services** et **Computers**, puis sélectionnez **My Computer**.

Etape 5 Dans le menu **Action**, cliquez sur **Properties**.

Etape 6 Sélectionnez l'onglet **COM Security**.

Etape 7 Dans la partie **Access Permissions**, cliquez sur **Edit Default**.

Etape 8 Sélectionnez l'utilisateur ou le groupe nécessitant un accès DCOM.

Remarque : Si l'utilisateur ou le groupe nécessitant un accès DCOM n'est pas répertorié dans la liste des autorisations, vous devez ajouter l'utilisateur à la configuration.

Etape 9 Sélectionnez les cases des autorisations suivantes :

- **Local Access** - Sélectionnez la case **Allow**.
- **Remote Access** - Sélectionnez la case **Allow**.

Etape 10 Cliquez sur **OK**.

La fenêtre My Computer Properties s'affiche.

Etape 11 Dans la partie **Launch and Activation Permissions**, cliquez sur **Edit Default**.

Etape 12 Sélectionnez l'utilisateur ou le groupe nécessitant un accès DCOM.

Etape 13 Configurez les autorisations suivantes :

- **Local Launch** - Sélectionnez la case **Allow**.
- **Remote Launch** - Sélectionnez la case **Allow**.
- **Local Activation** - Sélectionnez la case **Allow**.
- **Remote Activation** - Sélectionnez la case **Allow**.

Etape 14 Cliquez sur **OK**.

Etape 15 Cliquez sur **OK**.

Etape 16 Fermez la fenêtre Component Services.

Vous pouvez maintenant configurer Windows Management Instrumentation (WMI) sur votre système Windows Server 2003.

Configuration de l'accès utilisateur WMI pour Server 2003

L'utilisateur ou le groupe configuré pour l'accès DCOM doit également disposer d'une autorisation Windows Management Instrumentation (WMI) pour pouvoir accéder aux journaux d'événements requis par QRadar.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 1 Tapez ce qui suit :

```
wmimgmt.msc
```

Etape 2 Cliquez sur **OK**.

La fenêtre Windows Management Infrastructure s'affiche.

Etape 3 Cliquez avec le bouton droit de la souris sur **WMI Control (Local)**, puis cliquez sur **Properties**.

Etape 4 Cliquez sur l'onglet **Security**.

Etape 5 Dans Namespace navigation, ouvrez **Root**.

Etape 6 Dans l'arborescence du menu, cliquez sur **CIMV2**.

Etape 7 Cliquez sur **Security**.

La fenêtre Security for ROOT\CIMV2 s'affiche.

Etape 8 Sélectionnez l'utilisateur ou le groupe nécessitant l'accès WMI.

Remarque : Si l'utilisateur ou le groupe nécessitant un accès WMI n'est pas répertorié dans la liste d'autorisations, vous devez ajouter l'utilisateur à la configuration.

Etape 9 Configurez les autorisations d'utilisateur suivantes :

- **Execute Methods** - Sélectionnez la case **Allow**.
- **Provider Write** - Sélectionnez la case **Allow**.
- **Enable Account** - Sélectionnez la case **Allow**.
- **Remote Enable** - Sélectionnez la case **Allow**.

Remarque : Si l'utilisateur ou le groupe en cours de configuration est un administrateur, les cases Autorisation sont peut-être déjà sélectionnées.

Etape 10 Cliquez sur **OK**.

Etape 11 Cliquez sur **OK** pour fermer la fenêtre My Computer Properties.

Vous devez envoyer une requête au système Windows Server 2003 pour les journaux d'événement ou de sécurité afin de terminer la configuration DCOM en vérifiant les communications WMI.

Configurez Windows Server 2008

Pour configurer DCOM sur Windows Server 2008, procédez comme suit :

1. Vérifiez que les services Windows Server 2008 requis sont lancés. Pour en savoir plus, voir **Services DCOM et WMI requis de Windows Server 2008**.
2. Activez DCOM pour Windows Server 2008. Pour plus d'informations, voir **Activation de DCOM pour Windows Server 2008**.
3. Configurez les communications DCOM pour Windows Server 2008. Pour en savoir plus, voir **Configuration des communications DCOM pour Windows Server 2008**.
4. Configurez des comptes utilisateurs pour DCOM. Pour en savoir plus, voir **Configuration des comptes utilisateur Windows Server 2008 pour DCOM**.
5. Configurez le pare-feu Windows Server 2008. Pour plus d'informations, voir **Configuration du pare-feu Windows Server 2008**.
6. Configurez WMI pour Windows Server 2008. Pour plus d'informations, voir **Configuration de l'accès utilisateur WMI pour Windows Server 2008**.
7. Testez la configuration WMI. Pour en savoir plus, voir **Vérification des communications WMI**.

Services DCOM et WMI requis de Windows Server 2008

Les services Windows suivants pour DCOM et WMI doivent être lancés et configurés pour un démarrage automatique :

- Serveur
- Registre à distance
- Windows Management Instrumentation

Vous devez configurer le serveur et les services de registre à distance pour un démarrage automatique.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
services.msc
```

Etape 3 Cliquez sur **OK**.

Etape 4 Dans le panneau Details, vérifiez que les services suivants sont lancés et définis pour un démarrage automatique :

- Serveur
- Registre à distance
- Windows Management Instrumentation

Etape 5 Pour modifier une propriété du service, cliquez avec le bouton droit de la souris sur le nom du service, puis cliquez sur **Properties**.

Etape 6 Dans la zone de liste **Startup type**, sélectionnez **Automatic**.

Etape 7 Si le statut de service ne démarre pas, cliquez sur **Start**.

Etape 8 Cliquez sur **OK**.

Etape 9 Fermez la fenêtre Services.

Vous pouvez maintenant activer DCOM sur votre système Windows Server 2008.

Activation de DCOM pour Windows Server 2008

Vous devez activer DCOM sur Windows Server 2008.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
dcomcnfg
```

Etape 3 Cliquez sur **OK**.

La fenêtre Component Services s'affiche.

Etape 4 Dans la partie **Component Services**, ouvrez **Computers**, puis cliquez sur **My Computer**.

Etape 5 Dans le menu **Action**, cliquez sur **Properties**.

Etape 6 Sélectionnez l'onglet **Propriétés par défaut**.

Etape 7 Configurez les propriétés par défaut suivantes :

- **a** Sélectionnez la case **Enable Distributed COM on this computer**.
- **b** A l'aide de la zone de liste **Default Authentication Level**, sélectionnez **Connecter**.
- **c** A l'aide de la zone de liste **Default Impersonation Level**, sélectionnez **Identifier**.

Etape 8 Cliquez sur **OK**.

Etape 9 Cliquez sur **OK**.

Etape 10 Fermez la fenêtre Component Services.

Vous pouvez maintenant configurer les ports DCOM sur votre système Windows Server 2008.

Configuration des communications DCOM pour Windows Server 2008

Communications TCP/IP de Windows Server 2008 requis pour DCOM.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
dcomcnfg
```

Etape 3 Cliquez sur **OK**.

La fenêtre Component Services s'affiche.

Etape 4 Dans la partie Component Services, ouvrez **Component Services**, puis **Computers** et cliquez sur **My Computer**.

Etape 5 Dans le menu **Action**, cliquez sur **Properties**.

Etape 6 Sélectionnez l'onglet **Default Protocols**.

Etape 7 Configurez les options suivantes :

a Si Connection-oriented TCP/IP est répertorié dans la fenêtre DCOM Protocols, accédez à l'étape **d**.

b Si Connection-oriented TCP/IP n'est pas répertorié dans la fenêtre DCOM Protocol, sélectionnez **Add**.

La fenêtre de protocole Select DCOM s'affiche.

c Dans la zone de liste **Protocol Sequence**, sélectionnez **Connection-oriented TC/IP**.

d Cliquez sur **OK**.

La fenêtre My Computer Properties s'affiche.

Etape 8 Cliquez sur **OK**.

Etape 9 Fermez la fenêtre Component Services.

Vous pouvez maintenant configurer un compte utilisateur avec l'autorisation d'accéder à l'hôte.

Configuration des comptes utilisateur Windows Server 2008 pour DCOM

Après avoir activé DCOM, vous devez attribuer au compte une autorisation d'accès à DCOM sur l'hôte. Vous devez sélectionner un compte existant avec accès administrateur ou créer un compte utilisateur normal membre d'un groupe administrateur afin d'accéder à l'hôte.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
dcomcnfg
```

Etape 3 Cliquez sur **OK**.

La fenêtre Component Services s'affiche.

Etape 4 Dans la partie Console root, ouvrez **Component Services**, puis **Computers** et sélectionnez **My Computer**.

Etape 5 Dans le menu **Action**, cliquez sur **Properties**.

Etape 6 Sélectionnez l'onglet **COM Security**.

Etape 7 Dans **Access Permissions**, cliquez sur **Edit Default**.

Etape 8 Sélectionnez l'utilisateur ou le groupe nécessitant un accès DCOM.

Remarque : Si l'utilisateur ou le groupe nécessitant un accès DCOM n'est pas répertorié dans la liste des autorisations, vous devez ajouter l'utilisateur à la configuration.

Etape 9 Configurez les autorisations d'utilisateur suivantes :

- **Local Access** - Sélectionnez la case **Allow**.
- **Remote Access** - Sélectionnez la case **Allow**.

Etape 10 Cliquez sur **OK**.

La fenêtre My Computer Properties s'affiche.

Etape 11 Dans la partie **Launch and Activation Permissions**, cliquez sur **Edit Default**.

Etape 12 Sélectionnez l'utilisateur ou le groupe nécessitant un accès DCOM.

Remarque : Si l'utilisateur ou le groupe nécessitant un accès DCOM n'est pas répertorié dans la liste des autorisations, vous devez ajouter l'utilisateur à la configuration.

Etape 13 Configurez les autorisations d'utilisateur suivantes :

- **Local Launch** - Sélectionnez la case **Allow**.
- **Remote Launch** - Sélectionnez la case **Allow**.
- **Local Activation** - Sélectionnez la case **Allow**.
- **Remote Activation** - Sélectionnez la case **Allow**.

Etape 14 Cliquez sur **OK**.

Etape 15 Cliquez sur **OK**.

Etape 16 Fermez la fenêtre Component Services.

Vous pouvez maintenant configurer le pare-feu sous Windows Server 2008. Pour en savoir plus, voir **Configuration du pare-feu Windows Server 2008**.

Configuration du pare-feu Windows Server 2008

Si vous utilisez le pare-feu Windows Server 2008 sur un pare-feu situé entre Windows Server 2008 et QRadar, vous devez configurer le pare-feu avec une exception pour autoriser les communications DCOM.

Remarque : Vous devez être un administrateur pour pouvoir modifier les paramètres de pare-feu Windows ou pour y ajouter une exception.

Procédure

Etape 1 Cliquez sur **Start > All Programs > Administrative Tools > Server Manager**.

Etape 2 Dans le menu Server Manager, ouvrez **Configuration**, puis **Windows Firewall with Advanced Security**.

Etape 3 Sélectionnez **Inbound Rules**.

Etape 4 Dans le menu **Action**, cliquez sur **New Rule**.

Etape 5 Sélectionnez **Custom**, puis cliquez sur **Next**.

La fenêtre Program s'affiche.

Etape 6 Sélectionnez **All programs**, puis cliquez sur **Next**.

La fenêtre Protocol and Ports s'affiche.

Etape 7 Dans la zone de liste **Protocol type** list, sélectionnez **TCP** puis cliquez sur **Next**.

Remarque : Nous vous recommandons de ne pas limiter les ports locaux et à distance ou les adresses IP locales, mais de définir les règles de connexion de pare-feu par une adresse IP à distance.

Etape 8 Dans la partie **Which remote IP addresses does this rule apply to?**, sélectionnez **These IP addresses**.

Etape 9 Sélectionnez **These IP addresses**, puis cliquez sur **Add**.

La fenêtre IP Address s'affiche.

Etape 10 Dans la zone de saisie **This IP address or subnet**, tapez l'adresse IP de QRadar, cliquez sur **OK**.

La fenêtre Action s'affiche.

Etape 11 Sélectionnez **Allow the connection**, cliquez sur **Next**.

Etape 12 Entrez le profil de réseau auquel la règle s'applique, cliquez sur **Next**.

Etape 13 Tapez un nom et une description pour la règle de pare-feu, cliquez sur **Finish**.

Etape 14 Fermez cette fenêtre.

Vous pouvez maintenant configurer Windows Management Instrumentation (WMI) sur votre système Windows Server 2008.

Configuration de l'accès utilisateur WMI pour Windows Server 2008

L'utilisateur ou le groupe configuré pour l'accès DCOM doit également disposer d'une autorisation Windows Management Instrumentation (WMI) pour pouvoir accéder aux journaux d'événements requis par QRadar.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
wmimgmt.msc
```

Etape 3 Cliquez sur **OK**.

La fenêtre Windows Management Infrastructure s'affiche.

Etape 4 Cliquez avec le bouton droit de la souris sur **WMI Control (Local)**, puis sélectionnez **Properties**.

La fenêtre WMI Control (Local) Properties s'affiche.

Etape 5 Cliquez sur l'onglet **Security**.

Etape 6 Dans la partie **Namespace navigation**, ouvrez **Root**, puis cliquez sur **CIMV2**.

Etape 7 Cliquez sur **Security**.

La fenêtre Security for ROOT\CIMV2 s'affiche.

Etape 8 Sélectionnez l'utilisateur ou le groupe nécessitant l'accès WMI.

Remarque : Si l'utilisateur ou le groupe nécessitant un accès WMI n'est pas répertorié dans la liste d'autorisations, vous devez ajouter l'utilisateur à la configuration.

Etape 9 Sélectionnez les cases pour ajouter les permissions suivantes :

- **Execute Methods** - Sélectionnez la case **Allow**.
- **Provider Write** - Sélectionnez la case**Allow**.
- **Enable Account** - Sélectionnez la case **Allow**.
- **Remote Enable** - Sélectionnez la case **Allow**.

Remarque : Si l'utilisateur ou le groupe en cours de configuration est un administrateur système, les cases autorisation peuvent être sélectionnées.

Etape 10 Cliquez sur **OK**.

Etape 11 Cliquez sur **OK**.

Etape 12 Fermez la fenêtre WMIMGMT - WMI Control (Local).

Configuration de Windows Server 2008 R2 64-bit Trusted Installer

Windows Server 2008 R2 64-bit intègre une fonction de sécurité appelée Trusted Installer pouvant avoir un effet sur la connexion DCOM.

Procédure

Etape 1 Sur votre bureau, sélectionnez **Start > Run**.

Etape 2 Tapez ce qui suit :

```
regedit
```

Etape 3 Cliquez sur **OK**.

Remarque : Vous devez être un administrateur système pour pouvoir modifier les paramètres de registre.

La fenêtre Registry Editor s'affiche.

Etape 4 Accédez à l'emplacement de registre suivant :

```
HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
```

Etape 5 Cliquez avec le bouton droit de la souris sur l'entrée `{76A64158-CB41-11D1-8B02-00600806D9B6}`, puis cliquez sur **Permissions**.

Etape 6 Cliquez sur **Advanced**.

Etape 7 Cliquez sur l'onglet **Owner**.

Trusted Installer s'affiche en tant que propriétaire actuel.

Etape 8 Sélectionnez le groupe **Administrators**, cliquez sur **OK**.

Etape 9 Sélectionnez l'utilisateur QRadar, sélectionnez la case **Allow** pour obtenir une autorisation **Full Control**, puis cliquez sur **Apply**.

Remarque : Si l'utilisateur QRadar n'est pas répertorié dans la liste d'autorisation, vous devez ajouter l'utilisateur à la configuration.

Etape 10 Cliquez sur **Advanced**.

Etape 11 Cliquez sur l'onglet **Owner**.

Administrators s'affiche en tant que propriétaire actuel.

Etape 12 Sélectionnez ou ajoutez votre utilisateur QRadar, puis cliquez sur **OK**.

Remarque : Si l'utilisateur QRadar n'est pas répertorié dans la liste Change owner to permission, vous devez sélectionner la partie **Other users or groups** pour ajouter l'utilisateur à la configuration.

Etape 13 Cliquez sur **OK** pour retourner à Registry Editor.

Etape 14 Répétez **Etape 5** à **Etape 13** pour la clé de registre suivante :

```
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
```

Etape 15 Fermez la fenêtre Registry Editor.

Vous devez vérifier les communications WMI en envoyant une requête à Windows Server 2008 pour obtenir le journal d'événements de sécurité afin de terminer votre configuration DCOM.

Vérification des communications WMI

Pour vous aider dans la vérification de vos communications WMI, le RPM du protocole du journal des événements Microsoft Windows offre un outil test permettant à QRadar de transmettre des requêtes au serveur distant afin d'obtenir des informations sur le journal des événements Windows.

Pour utiliser cet outil test, votre système doit exécuter la dernière version du protocole du journal des événements Windows.

Procédure

Etape 1 A l'aide de Secure Shell, connectez-vous à QRadar en tant que superutilisateur.

Nom d'utilisateur : `root`

Mot de passe : `<password>`

Etape 2 Entrez la commande suivante :

```
cd /opt/qradar/jars
```

Etape 3 Entrez la commande suivante :

```
java -jar WMITestTool-<date>.jar
```

Où `<date>` est la date de publication de l'outil de test WMI.

Etape 4 Configurez les paramètres suivants :

a **Remote Windows Host** - Tapez l'adresse IP de votre serveur Windows.

b **Active Directory Domain, or Hostname if in a Workgroup** - Tapez le domaine ou le groupe de travail de votre serveur Windows.

c **Username** - Tapez le nom d'utilisateur requis pour accéder au serveur Windows à distance.

d **Password** - Tapez le nom d'utilisateur requis pour accéder au serveur Windows à distance.

L'outil test tente de se connecter à votre serveur Windows à distance.

Etape 5 Dans les paramètres **WQL Query**, tapez ce qui suit :

```
Select NumberOfRecords From Win32_NTEventLogFile WHERE
LogFileName='Security'
```

Remarque : L'exemple fournit des fonctions avec des versions à 32 bits et 64 bits de Windows Server 2003 et Windows Server 2008.

Si QRadar peut normalement accéder à votre serveur Windows, les résultats du journal des événements de sécurité sont renvoyés.

Par exemple :

```
-----
exemple de Win32_NTEventlogFile
Nom = C:\Windows\System32\Winevt\Logs\Security.evtx
Nombre d'enregistrements = 5786
-----
```

Si la requête renvoyée affiche un nombre total d'enregistrements = 0, ou si une erreur se produit, vous devez vérifier les services en cours d'exécution, votre configuration DCOM et WMI ainsi que les paramètres de pare-feu. Une fois la configuration de votre serveur Windows vérifiée, contactez le centre d'assistance.

Si vous rencontrez des problèmes de connexion, utilisez l'outil test ainsi que le pare-feu Windows temporairement désactivé. Si l'outil test renvoie les résultats d'événements de sécurité, activez le pare-feu Windows, puis consultez votre administrateur de réseau.

D AVIS ET MARQUES

Contenu de cette annexe :

Cette section contient des informations relatives aux consignes de sécurité, aux marques et à la conformité.

Avis

Ces informations ont été développées pour des produits et des services proposés aux Etats-Unis.

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 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. 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 plus d'informations sur les licences concernant les produits utilisant un jeu de caractères double octet, contactez le département IBM Intellectual Property Department de votre pays ou envoyez une demande 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 paragraphe suivant ne s'applique ni au Royaume-Uni, ni à aucun pays dans lequel il serait contraire aux lois locales : 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.

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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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 indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente 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. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.. Les autres noms de produit et de service peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM (Informations relatives au copyright) est disponible sur le Web à l'adresse *www.ibm.com/legal/copytrade.shtml*.

Les termes qui suivent sont des marques d'autres sociétés :

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques de Oracle et/ou de ses affiliés.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

INDEX

S

T

V

W