IBM Security QRadar Risk Manager
Version 7.2.2

Guide de configuration d'adaptateur

SC43-0365-01

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 39.

Deuxième édition - Juillet 2014

Réf. US : SC27-6248-01

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Introduction à la configuration d'adaptateurs pour QRadar Risk Manager

IBM® Security QRadar Risk Manager est un dispositif utilisé pour surveiller des configurations d'unité, simuler des modifications apportées à votre environnement réseau, et hiérarchiser les risques et vulnérabilités.

Utilisateurs concernés

Les administrateurs de réseau qui sont responsables de l'installation et de la configuration d'adaptateurs doivent bien maîtriser les concepts de sécurité réseau et les configurations d'unité.

Documentation technique

Pour rechercher la documentation produit IBM Security QRadar sur le Web, y compris toute la documentation traduite, accédez àIBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Pour savoir comment accéder à plus de documentation technique dans la bibliothèque produit QRadar, voir Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Déclaration de pratiques de sécurité recommandées

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

Chapitre 1. Présentation des adaptateurs

Utilisez des adaptateurs pour intégrer IBM Security QRadar Risk Manager à vos unités réseau. La configuration d'adaptateurs permet à QRadar Risk Manager d'interroger et d'importer les paramètres de configuration des unités réseau (pare-feu, routeurs et commutateurs, par exemple).

Remarque : Vous ne pouvez pas importer des unités qui utilisent un IP de serveur de gestion, par exemple, CPSMS et IBM Internet Security Systems GX.

Topologie de réseau et configuration

QRadar Risk Manager utilise de adaptateurs pour collecter des configurations de réseau. Les adaptateurs transforment les informations de configuration en un format unifié pour tous les modèles d'unité pris en charge, fabricants et types. QRadar Risk Manager utilise les données pour appréhender votre topologie réseau et la configuration de vos unités réseau.

Pour connecter des unités externes du réseau, QRadar Risk Manager doit être capable d'accéder aux unités. QRadar Risk Manager utilise des données d'identification utilisateur configurées afin d'accéder à l'unité et de télécharger des configurations.

Processus d'intégration d'unités réseau

Pour intégrer des unités réseau à QRadar Risk Manager, procédez comme suit :

1. Configurez votre unité réseau avec l'accès approprié à QRadar Risk Manager.
2. Installez l'adaptateur approprié à votre unité réseau sur votre dispositif QRadar Risk Manager.
3. Utilisez la gestion de sources de configuration (Configuration Source Management) pour ajouter vos unités réseau à QRadar Risk Manager.
4. Définissez la méthode de communication (protocole) requise pour la communication avec vos unités réseau.

   Pour plus d'informations, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Si QRadar Risk Manager et vos unités réseau ne parviennent pas à communiquer, reportez-vous aux informations du kit d'outils de configuration en mode déconnecté dans le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Types d'adaptateur

IBM Security QRadar Risk Manager prend en charge plusieurs types d'adaptateur.

Les adaptateurs suivants sont pris en charge :

- BIG-IP
- Check Point SecurePlatform Appliances
- Cisco Internet Operating System (IOS)
- Cisco Catalyst (CatOS)
- Check Point Security Management Server

- Cisco Security Appliances
- HP Networking ProVision
- Juniper Networks ScreenOS
- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto

Chapitre 2. Installation d'un adaptateur

Vous devez télécharger un adaptateur sur votre console IBM Security QRadar SIEM Console, puis copier les fichiers d'adaptateur dans IBM Security QRadar Risk Manager.

Avant de commencer

Vous accédez et téléchargez des adaptateurs depuis le site Fix Central (www.ibm.com/support/fixcentral/). Les fichiers RPM sont inclus dans le téléchargement.

Après que vous avez établi la connexion initiale, QRadar SIEM Console est la seule unité qui peut communiquer directement avec QRadar Risk Manager.

Procédure

1. En utilisant Secure Shell (SSH), connectez-vous à votre console QRadar SIEM Console en tan qu'utilisateur root.
2. Téléchargez le fichier d'adaptateur depuis le site Web du support IBM (www.ibm.com/support) sur votre console QRadar SIEM Console.
3. Pour compier le fichier d'adaptateur depuis votre console QRadar SIEM Console dans QRadar Risk Manager, tapez la commande suivante :

   `scp` *`adaptateur`*`.rpm root@`*`adresse IP`*

   L'*adresse IP* correspond à l'adresse IP ou au nom d'hôte de QRadar Risk Manager.

   Exemple : `scp adapters.cisco.ios-2011_05-205181.noarch.rpm root@100.100.100.100:`
4. Sur votre dispositif QRadar Risk Manager, entrez le mot de passe de l'utilisateur root.
5. En utilisant SSH depuis votre console QRadar SIEM Console, connectez-vous à votre dispositif QRadar Risk Manager en tant qu'utilisateur root.
6. Depuis le répertoire racine (root) qui contient le fichier d'adaptateur, tapez la commande suivante pour installer l'adaptateur :

   `rpm -Uvh` *`nom-fichier_RPM`*

   Exemple : `rpm -Uvh adapters.cisco.ios-2011_05-205181.noarch.rpm`
7. Pour redémarrer les services pour le serveur ziptie et terminer l'installation, tapez la commande suivante :

   `service ziptie-server restart`

   Important : Le redémarrage des services pour le serveur ziptie interrompt toute sauvegarde en cours depuis la gestion de sources de configuration (Configuration Source Management).

Désinstallation d'un adaptateur

Utilisez la commande **rpm** pour retirer un adaptateur de IBM Security QRadar Risk Manager.

Procédure

1. En utilisant Secure Shell (SSH), connectez-vous à la console IBM Security QRadar SIEM Console en tan qu'utilisateur root.
2. Pour désinstaller un adaptateur, tapez la commande suivante :

   `rpm -e` *`fichier d'adaptateur`*

   Exemple : `rpm -e adapters.cisco.ios-2011_05-205181.noarch.rpm`

Chapitre 3. Méthodes d'ajout d'unités réseau

Utilisez la gestion de sources de configuration (Configuration Source Management) pour ajouter des unités réseau à IBM Security QRadar Risk Manager.

Le tableau suivant répertorie les méthodes que vous pouvez utiliser pour ajouter une unité réseau.

Tableau 1. Méthodes d'ajout d'une unité réseau à QRadar Risk Manager

Méthode	Description
Add Device	Ajoutez une unité.
Discover Devices	Ajoutez plusieurs unités.
Discover NSM	Ajoutez des unités gérées par une console NSM Juniper Networks.
Discover CPSMS From SiteProtector	Ajoutez des unités gérées par un serveur Check Point Security Manager Server (CPSMS).
Discover	Ajoutez des unités depuis SiteProtector.

Ajout d'une unité réseau

Pour ajouter une unité réseau à IBM Security QRadar Risk Manager, utilisez la gestion de sources de configuration (Configuration Source Management).

Avant de commencer

Vérifiez les versions logicielles prises en charge, les données d'identification, ainsi que les commandes requises pour vos unités réseau. Pour plus d'informations, voir Chapitre 4, «Adaptateurs pris en charge», à la page 11.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins**
3. Dans le volet Risk Manager, cliquez sur Configuration Source Management.
4. Dans le menu de navigation, cliquez sur **Credentials**.
5. Dans le volet Network Groups, cliquez sur **Add a new network group**.
   a. Indiquez un nom pour le groupe de réseau et cliquez sur **OK**.
   b. Tapez l'adresse IP de votre unité puis cliquez sur **Add**.

      Vous pouvez taper une adresse IP, une plage d'adresses IP, un sous-réseau CIDR ou un caractère générique. Pour utiliser un caractère générique, tapez `10.1.*.*`, ou pour un routage CIDR, tapez `10.2.1.0/24`.

      Restriction : Ne répliquez pas des adresses d'unité qui existent dans d'autres groupes de réseau de Configuration Source Management.
   c. Assurez-vous que les adresses que vous ajoutez s'affichent dans la zone **Network address**, sous la zone **Add address**.
   d. Répétez les deux étapes précédentes pour chaque adresse IP à ajouter.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.

a. Indiquez un nom pour l'ensemble de données d'identification et cliquez sur **OK**.
b. Sélectionnez le nom de l'ensemble de données d'identification que vous avez créé, puis entrez des valeurs pour les paramètres.

   Le tableau suivant décrit ces paramètres.

Tableau 2. Options de paramètre pour les données d'identification

Paramètre	Description
Username	Nom d'utilisateur valide permettant de se connecter à l'adaptateur. Pour les adaptateurs, le nom d'utilisateur et le mot de passe fournis nécessitent l'accès à plusieurs fichiers tels que les suivants : • `rule.C` • `objects.C` • `implied_rules.C` • `Standard.PF`
Password	Mot de passe de l'unité.
Enable Password	Mot de passe pour l'authentification de second niveau. Ce mot de passe est obligatoire pour l'invite de saisie des données d'identification nécessaires à l'utilisateur pour le mode expert.
SNMP Get Community	Facultatif
SNMPv3 Authentication Username	Facultatif
SNMPv3 Authentication Password	Facultatif
SNMPv3 Privacy Password	Facultatif Protocole utilisé pour déchiffrer les messages d'alerte SNMPv3.

Restriction : Si votre unité réseau satisfait l'une des conditions suivantes, vous devez configurer des protocoles dans la gestion de sources de configuration :

- Votre unité utilise un port non standard pour le protocole de communication.
- Vous souhaitez configurer le protocole utilisé par IBM Security QRadar Risk Manager pour communiquer avec des adresses IP spécifiques.

Vous trouverez des informations supplémentaires sur la configuration de sources dans le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

7. Dans le menu de navigation, ajoutez une unité.
   - Pour ajouter une unité réseau, cliquez sur **Add Device**.
   - Pour ajouter plusieurs adresses IP pour des unités réseau, sélectionnez **Discover Devices**.
8. Entrez l'adresse IP de l'unité et sélectionnez le type d'adaptateur, puis cliquez sur **Add**.

Un point d'interrogation bleu s'affiche dans la liste des unités pour les unités qui ne sont pas sauvegardées.

9. Sélectionnez l'unité que vous venez d'ajouter à la liste des unités, puis cliquez sur **Backup**.
10. Répétez cette procédure pour chaque type d'unité réseau à ajouter.

Que faire ensuite

Une fois toutes les unités requises ajoutées, vous pouvez configurer des protocoles. Pour plus d'informations, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Ajout d'unités gérées par une console Juniper Networks NSM

Utilisez la gestion de sources de configuration (Configuration Source Management) pour ajouter à IBM Security QRadar Risk Manager toutes les unités depuis une console Juniper Networks NSM.

Avant de commencer

Vérifiez les versions logicielles prises en charge, les données d'identification, ainsi que les commandes requises pour vos unités réseau. Pour plus d'informations, voir Chapitre 4, «Adaptateurs pris en charge», à la page 11.

Procédure

1. Dans IBM Security QRadar SIEM, cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins**
3. Dans le volet Risk Manager, cliquez sur **Configuration Source Management**.
4. Dans le menu de navigation, cliquez sur **Credentials**.
5. Dans le volet Network Groups, cliquez sur **Add a new network group**.
   a. Indiquez un nom pour le groupe de réseau et cliquez sur **OK**.
   b. Tapez l'adresse IP de votre unité puis cliquez sur **Add**.

      Vous pouvez taper une adresse IP, une plage d'adresses IP, un sous-réseau CIDR ou un caractère générique. Pour utiliser un caractère générique, tapez `10.1.*.*`, ou pour un routage CIDR, tapez `10.2.1.0/24`.

      Restriction : Ne répliquez pas des adresses d'unité qui existent dans d'autres groupes de réseau de Configuration Source Management.
   c. Assurez-vous que les adresses que vous ajoutez s'affichent dans la zone **Network address**, sous la zone **Add address**.
   d. Répétez les deux étapes précédentes pour chaque adresse IP à ajouter.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
   a. Indiquez un nom pour l'ensemble de données d'identification et cliquez sur **OK**.
   b. Sélectionnez le nom de l'ensemble de données d'identification que vous avez créé, puis entrez des valeurs pour les paramètres.

      Le tableau suivant décrit ces paramètres.

Tableau 3. Options de paramètre pour les données d'identification de service Web Juniper NSM

Paramètre	Description
Username	Nom d'utilisateur valide permettant de se connecter aux services Web Juniper NSM. Pour les services Web Juniper NSM, cet utilisateur doit être capable d'accéder au serveur Juniper NSM.
Password	Mot de passe de l'unité.
Enable Password	Facultatif.

Restriction : Juniper Networks NSM ne prend pas en charge le protocole SNMP.

7. Dans le menu de navigation, cliquez sur **Discover from NSM**.
8. Entrez des valeurs pour l'adresse IP et les données d'identification de l'utilisateur, cliquez sur **OK** puis cliquez sur **GO**.
9. Sélectionnez l'unité que vous venez d'ajouter à la liste des unités, puis cliquez sur **Backup** puis sur **Yes**.

Que faire ensuite

Une fois toutes les unités requises ajoutées, vous pouvez configurer des protocoles. Pour plus d'informations, reportez-vous au manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Ajout d'unités gérées par une console CPSMS

Utilisez la gestion de sources de configuration (Configuration Source Management) pour ajouter toutes les unités à IBM Security QRadar Risk Manager depuis un serveur CPSMS (Check Point Security Manager Server).

Avant de commencer

Vérifiez les versions logicielles prises en charge, les données d'identification, ainsi que les commandes requises pour vos unités réseau. Pour plus d'informations, voir Chapitre 4, «Adaptateurs pris en charge», à la page 11.

Vous devez vous procurer le nom OPSEC Entity SIC, le nom OPSEC Application Object SIC et le mot de passe à utilisation unique pour Pull Certificate avant de débuter cette procédure. Pour plus d'informations, reportez-vous à votre documentation CPSMS.

Remarque : La fonctions d'importation d'unité (Device Import) n'est pas compatible avec les adaptateurs CPSMS.

Pourquoi et quand exécuter cette tâche

Vous devez répéter cette procédure pour chaque serveur CPSMS que vous souhaitez contacter pour lancer la reconnaissance de ses pare-feu gérés.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins**
3. Dans le volet Risk Manager, cliquez sur Configuration Source Management.
4. Dans le menu de navigation, cliquez sur **Credentials**.
5. Dans le volet Network Groups, cliquez sur **Add a new network group**.
   a. Indiquez un nom pour le groupe de réseau et cliquez sur **OK**.
   b. Tapez l'adresse IP de votre unité CPSMS puis cliquez sur **Add**.

      Restriction : Ne répliquez pas des adresses d'unité qui existent dans d'autres groupes de réseau de Configuration Source Management.
   c. Assurez-vous que les adresses que vous ajoutez s'affichent dans la zone **Network address**, sous la zone **Add address**.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
   a. Indiquez un nom pour l'ensemble de données d'identification et cliquez sur **OK**.
   b. Sélectionnez le nom de l'ensemble de données d'identification que vous avez créé et tapez un nom d'utilisateur et un mot de passe valides pour l'unité.
7. Tapez le nom OPSEC Entity SIC du serveur CPSMS qui gère les unités de pare-feu à reconnaître. Exemple : `CN=cp_mgmt_vm230-cpsms2-gw3,O=vm226-CPSMS..bs7ocx`
8. Tapez le nom OPSEC Application Object SIC qui a été créé, à l'aide de l'application Check Point SmartDashboard, sur le serveur CPSM. Exemple : `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
9. Procurez-vous le certificat OPSEC SSL :
   a. Cliquez sur **Get Certificate**.
   b. Dans la zone **Certificate Authority IP**, tapez l'adresse IP.
   c. Dans la zone **Pull Certificate Password**, tapez le mot de passe à utilisation unique pour l'application OPSEC.
   d. Cliquez sur **OK**.
10. Cliquez sur **OK**.
11. Cliquez sur **Discover From Check Point SMS**, puis indiquez l'adresse IP du serveur CPSMS.
12. Cliquez sur OK.
13. Répétez cette procédure pour chaque unité CPSMS à ajouter.

Que faire ensuite

Une fois toutes les unités requises ajoutées, vous pouvez sauvegarder vos unités et les afficher dans la topologie.

Ajout d'unités gérées par SiteProtector

Utilisez la gestion de sources de configuration (Configuration Source Management) pour ajouter des unités depuis SiteProtector à IBM Security QRadar Risk Manager.

Avant de commencer

Les adaptateurs IBM Internet Security Systems GX et IBM Security SiteProtector System doivent être installés pour que vous puissiez ajouter des unités.

Le protocole Microsoft SQL doit être activé pour l'utilisation du port 1433 de Microsoft SQL Server.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins**.
3. Dans le volet Risk Manager, cliquez sur Configuration Source Management.
4. Dans le menu de navigation, cliquez sur **Credentials**.
5. Dans le volet Network Groups, cliquez sur **Add a new network group**.
   a. Indiquez un nom pour le groupe de réseau et cliquez sur **OK**.
   b. Tapez l'adresse IP de votre unité SiteProtector puis cliquez sur **Add**.
   c. Assurez-vous que les adresses que vous ajoutez s'affichent dans la zone **Network address**, sous la zone **Add address**.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
   a. Indiquez un nom pour l'ensemble de données d'identification et cliquez sur **OK**.
   b. Sélectionnez le nom de l'ensemble de données d'identification que vous avez créé et tapez un nom d'utilisateur et un mot de passe valides pour l'unité.

      Restriction : Le nom d'utilisateur et le mot de passe sont identiques aux données d'identifications utilisées pour accéder à la base de données Microsoft SQL Server de SiteProtector.
7. Cliquez sur **OK**.
8. Cliquez sur **Discover From SiteProtector**, puis entrez l'adresse IP SiteProtector.
9. Cliquez sur **OK**.

Que faire ensuite

Une fois toutes les unités requises ajoutées, vous pouvez sauvegarder vos unités et les afficher dans la topologie.

Chapitre 4. Adaptateurs pris en charge

IBM Security QRadar Risk Manager s'intègre aux produits de sécurité de nombreux fabricants et vendeurs.

La liste des adaptateurs pris en charge et la documentation qui s'y rapporte ne cessent de croître. Si un adaptateur pour votre unité réseau ne figure pas dans la liste, prenez contact avec votre ingénieur commercial IBM.

Les informations suivantes sont fournies pour chaque adaptateur pris en charge :

Versions prises en charge

Indique le nom du produit et la version prise en charge.

Prend en charge les données de voisinage

Indique si les données de voisinage sont prises en charge pour cet adaptateur. Si votre unité prend en charge les données de voisinage, vous obtenez ces données à partir d'une unité en utilisant le protocole SNMP (Simple Network Management Protocol) et une interface de ligne de commande.

Reconnaissance SNMP

Indique si l'unité autorise la reconnaissance via SNMP.

Les unités SNMP génériques ne disposent pas de routes et, de ce fait, ne transmettent pas le trafic.

Paramètres de données d'identification obligatoires

Indique les conditions d'accès nécessaires pour que QRadar Risk Manager et l'unité puissent se connecter.

Vous pouvez utiliser la gestion de source de configuration (Configuration Source Management) pour configurer les données d'identification d'unité. Assurez-vous que ces données qui sont configurées dans QRadar Risk Manager et sur l'unité sont identiques.

Si un paramètre est facultatif, vous pouvez laisser la zone à blanc.

Protocoles de connexion

Indique les protocoles pris en charge pour l'unité réseau.

Commandes requises

Indique la liste des commandes requises par l'adaptateur pour la connexion et la collecte de données.

Pour exécuter les commandes répertoriées pour un adaptateur, les données d'identification fournies dans QRadar Risk Manager doivent disposer des droits appropriés.

Fichiers collectés

Indique la liste des fichiers auxquels l'adaptateur doit pouvoir avoir accès. Pour accéder à ces fichiers, les droits appropriés doivent être configurés pour l'adaptateur.

BIG-IP

IBM Security QRadar Risk Manager prend en charge l'adaptateur BIG-IP.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur BIG-IP.

Tableau 4. Exigences d'intégration pour l'adaptateur BIG-IP

Exigence d'intégration	Description
Versions	BIG-IP version 10 et ultérieure.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à BIG-IP dans SNMP sysDescr.

Paramètres de données d'identification obligatoires	`Username`
	
	`Password`

Protocoles de connexion	Telnet SSH

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`cat filename`
	
	`dmesg`
	
	`uptime`
	
	`route -n`
	
	`ip addr list`
	
	`snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.1`
	
	`snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.2`

Tableau 4. Exigences d'intégration pour l'adaptateur BIG-IP (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données bigpipe	`bigpipe global`
	`bigpipe system hostname`
	`bigpipe platform`
	`bigpipe version show`
	`bigpipe db packetfilter`
	`bigpipe db packetfilter.defaultaction`
	`bigpipe packet filter list`
	`bigpipe nat list all`
	`bigpipe vlan show all`
	`bigpipe vlangroup list all`
	`bigpipe vlangroup`
	`bigpipe interface show all`
	`bigpipe interface all media speed`
	`bigpipe trunk all interfaces`
	`bigpipe stp show all`
	`bigpipe route all list all`
	`bigpipe mgmt show all`
	`bigpipe mgmt route show all`
	`bigpipe pool`
	`bigpipe self`
	`bigpipe virtual list all`
	`bigpipe snat list all`
	`bigpipe snatpool list all`

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`b db snat.anyipprotocol`

Tableau 4. Exigences d'intégration pour l'adaptateur BIG-IP (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données tmsh	`tmsh -q list sys global-settings hostname`
	
	`tmsh -q show sys version`
	
	`tmsh -q show sys hardware`
	
	`tmsh -q list sys snmp sys-contact`
	
	`tmsh -q show sys memory`
	
	`tmsh -q list /net interface all-properties`
	
	`tmsh -q list net trunk`
	
	`tmsh -q list /sys db packetfilter`
	
	`tmsh -q list /sys db packetfilter.defaultaction`
	
	`tmsh -q list /net packet-filter`
	
	`tmsh -q list /net vlan all-properties`
	
	`tmsh -q show /net vlan`
	
	`tmsh -q list /net vlan-group all all-properties`
	
	`tmsh -q list net tunnels`

Tableau 4. Exigences d'intégration pour l'adaptateur BIG-IP (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données tmsh (suite)	`tmsh -q show /net vlan-group`
	`tmsh -q list ltm virtual`
	`tmsh -q list ltm nat`
	`tmsh -q list ltm snatpool`
	`tmsh -q list ltm snat`
	`tmsh -q list sys db snat.anyipprotocol`
	`tmsh -q list net stp-globals all-properties`
	`tmsh -q list net stp priority`
	`tmsh -q list net stp all-properties`
	`tmsh -q list net route`
	`tmsh -q list sys management-ip`
	`tmsh -q list sys management-route`
	`tmsh -q list ltm pool`
	`tmsh -q list net self`
	`tmsh -q list net ipsec`

Fichiers collectés	`/config/bigip.license`
	`/config/snmp/snmpd.conf`
	`/etc/passwd`

Check Point SecurePlatform Appliances

IBM Security QRadar Risk Manager prend en charge l'adaptateur Check Point SecurePlatform Appliances.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Check Point SecurePlatform Appliances.

Tableau 5. Exigences d'intégration pour l'adaptateur Check Point SecurePlatform Appliances

Exigence d'intégration	Description
Versions	Versions R65 et ultérieures **Restriction :** Les dispositifs Nokia IPSO ne sont pas pris en charge pour la sauvegarde.
Prise en charge des données de voisinage	Pas de prise en charge
Reconnaissance SNMP	Correspond à NGX dans SNMP sysDescr.

Tableau 5. Exigences d'intégration pour l'adaptateur Check Point SecurePlatform Appliances (suite)

Exigence d'intégration	Description
Paramètres de données d'identification obligatoires	Username Password Enable Password (mode expert)
Protocoles de connexion	Telnet SSH
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	hostname dmidecode ver uptime dmesg route -n show users ifconfig -a echo $FWDIR
Fichiers collectés	rules.C objects.C implied_rules.C Standard.pf snmpd.com

Adaptateur Check Point Security Management Server

Vous utilisez l'adaptateur Check Point Security Management Server (CPSMS) pour reconnaître et sauvegarder les noeuds d'extrémités gérés par le serveur de gestion de la sécurité des points de contrôle (CPSMS). Ces noeuds d'extrémité sont utilisés pour exécuter CheckPoint FireWall-1 et la famille de produits VPN-1.

L'adaptateur CPSMS est basé sur la bibliothèque d'API de logiciel SDK CPMI OPSEC.

Transmission de compatibilité pour les connexions CPMI

Les connexions CPMI sont compatibles avec les versions les plus récentes. Par exemple, une application CPMI qui utilise un logiciel SDK NG FP3 OPSEC peut communiquer avec VPN-1 NGX R60.

Compatibilité avec les versions antérieures pour les connexions CPMI

Les connexions CPMI ne sont pas compatibles avec une version antérieure. Par exemple, une application CPMI utilisant OPSEC SDK 6.0 ne peut pas communiquer avec une version de VPN-1 antérieure à NGX R60.

Configuration requise pour CPSMS

Deux configurations requises doivent être disponibles pour CPSMS. Elles sont disponibles par défaut que CPSMS est installé ; vous devez vous assurer que ces configurations requises sont conservées.

L'application client de CPSMS, cpsms_client, se trouve sur l'adaptateur CPSMS. L'application cpsms_client établit avec CPSMS une méthode d'authentification asymétrique via un canal SICS (Secure Internal Communication). Cette méthode est également appelée méthode OPSEC_SSLCA.

La méthode d'authentification asymétrique est traduite en configuration requise. Vous devez configurer et activer la communication SIC sur le serveur de gestion de pare-feu afin d'autoriser l'application cpsms_client à communiquer avec CPSMS.

Les ports suivants doivent être ouverts sur le serveur CPSMS :

- Port 18190 pour le service Check Point Management Interface (CPMI)
- Port 18210 pour le service Check Point Internal CA Pull Certificate Service (FW1_ica_pull)

Si vous ne pouvez pas utiliser 18190 comme port d'écoute pour CPMI, le numéro de port de l'adaptateur CPSMS doit être similaire à la valeur indiquée dans le fichier `$FWDIR/conf/fwopsec.conf` pour l'interface CPMI sur le serveur CPSMS. Par exemple : cpmi_server auth_port 18190.

Pour autoriser le client cpsms_client à communiquer avec Check Point Management Server, le fichier `$CPDIR/conf/sic_policy.conf` sur CPSMS doit utiliser au minimum la ligne suivante :

```
# OPSEC applications default
ANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp
# sam proxy
ANY ; Modules, DN_Mgmt ; ANY; sam ; sslca
ANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_comp
ANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_comp
ANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp
```

Cisco CatOS

IBM Security QRadar Risk Manager prend en charge l'adaptateur Cisco Catalyst (CatOS).

L'adaptateur Cisco CatOS collecte les configurations d'unité en sauvegardant les appareils réseau CatOS visualisables par QRadar Risk Manager.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Cisco CatOS.

Tableau 6. Exigences d'intégration pour l'adaptateur Cisco CatOS

Exigence d'intégration	Description
Versions	Catalyst série 6500 - périphériques châssis. **Restriction :** L'adaptateur pour CatOS sauvegarde uniquement la structure de port de commutation essentielle. Les adaptateurs CatOS MSFC (Multilayer Switch Feature Card) sont sauvegardés par des adaptateurs Cisco IOS. Les adaptateurs CatOS (Firewall Services Module) sont sauvegardés par des adaptateurs Cisco ASA.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à CATOS ou Catalyst Operating System dans SNMP sysDescr.

Paramètres de données d'identification obligatoires	`Username`
	
	`Password`
	
	`Enable Password`

Protocoles de connexion	Telnet SSH

Tableau 6. Exigences d'intégration pour l'adaptateur Cisco CatOS (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`show version`
	`whichboot`
	`show module`
	`show mod ver`
	`show system`
	`show flash devices`
	`show flash ...`
	`show snmp ifalias`
	`show port ifindex`
	`show interface`
	`show port`
	`show spantree`
	`show ip route`
	`show vlan`
	`show vtp domain`
	`show arp`
	`show cdp`
	`show cam dynamic`
	`show port status`
	`show counters`

Cisco IOS

IBM Security QRadar Risk Manager prend en charge l'adaptateur Cisco Internet Operating System (IOS).

L'adaptateur Cisco IOS collecte les configurations d'unité en sauvegardant les commutateurs et routeurs réseau basés IOS.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Cisco IOS.

Tableau 7. Exigences d'intégration pour l'adaptateur Cisco IOS

Exigence d'intégration	Description
Versions	10.1 et versions ultérieures pour les routeurs et commutateurs Commutateurs Cisco Catalyst 6500 avec MSFC. Utilisez l'adaptateur Cisco IOS pour sauvegarder la configuration et l'état des services de carte MSFC. Si un routeur Cisco IOS série 7600 dispose d'un FWSM, utilisez l'adaptateur Cisco ASA pour sauvegarder le FWSM.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à ISO ou Cisco Internet Operation System dans SNMP sysDescr.

Paramètres de données d'identification obligatoires	`Username`
	
	`Password`
	
	`Enable Password`

Protocoles de connexion	Telnet SSH + SCP TFTP

Tableau 7. Exigences d'intégration pour l'adaptateur Cisco IOS (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`show access lists`
	`show cdp neighbors detail`
	`show eigrp neighbors`
	`show diagbus`
	`show diag`
	`show install running`
	`show interfaces`
	`show inventory`
	`show file systems`
	`show mac-address-table dynamic`
	`show module`
	`show mod version`
	`show power`
	`show startup-config`
	`show object-group`
	`show running-config`
	`show snmp`
	`show glbp`
	`show spanning-tree`
	`show standby`
	`set terminal length`
	`show vlan`
	`show vtp status`
	`show version`
	`show vrrp`

Tableau 7. Exigences d'intégration pour l'adaptateur Cisco IOS (suite)

Exigence d'intégration	Description

Commandes `show ip` nécessaires à l'adaptateur pour se connecter et collecter des données	`show ip arp`
	`show ip bgp neighbors`
	`show ip eigrp interface`
	`show ip eigrp neighbors`
	`show ip eigrp topology`
	`show ip ospf`
	`show ip ospf neighbor`
	`show ip protocols`
	`show ipv6 neighbors`
	`show ip ospf interface`
	`show ip route eigrp`

Cisco Nexus

Pour intégrer IBM Security QRadar Risk Manager à vos unités réseau, veillez à vérifier les exigences relatives à l'adaptateur Cisco Nexus.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Cisco Nexus.

Tableau 8. Exigences d'intégration pour l'adaptateur Cisco Nexus

Exigence d'intégration	Description
Versions	Aucune restriction de version
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à *Cisco NX-OS* et une chaîne de qualification facultative qui se termine par *Software* dans SNMP sysDescr. **Exemple :** *(Cisco NX\-OS.* Software)*

Paramètres de données d'identification obligatoires	`Username`
	`Password`
	`Enable Password`
	Si vous ajoutez des contextes d'unité virtuelle (VDC) en tant qu'unités individuelles, vérifiez que les données d'identification requises permettent d'exécuter les actions suivantes :
	• Accéder au compte activé pour les VDC.
	• Utiliser les commandes requises dans ce contexte virtuel.

Protocoles de connexion	Telnet SSH

Tableau 8. Exigences d'intégration pour l'adaptateur Cisco Nexus (suite)

Exigence d'intégration	Description

Fichiers tiers requis	`adapters-common-2013.03_05-515182.noarch.rpm`
	
	`perl-Net-CIDR-Set-0.11-1.noarch.rpm`
	
	`perl-XML-Twig-3.42-1.noarch.rpm`

Tableau 8. Exigences d'intégration pour l'adaptateur Cisco Nexus (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`terminal length 0`
	
	`show version`
	
	`show hostname`
	
	`show vdc`
	
	`snow snmp`
	
	`show module`
	
	`dir` *fs*(*fs* est le système de fichiers sur l'unité)
	
	`show interface brief`
	
	`show interface snmp-ifindex`
	
	`show interface` *if* (*if* correspond à toutes les interfaces de `show interface brief` avec des sections de configuration)
	
	`show running-config`
	
	`show startup-config`
	
	`show static-route`
	
	`show ip access-lists`
	
	`show object-group`
	
	`show vlan`
	
	`show vtp status`
	
	`show hsrp`
	
	`show vrrp`
	
	`show vtp`
	
	`show glbp`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`
	
	`show ipv6 route`
	
	`show ipv6 ndp`
	
	`show cdp entry all`
	
	`switchto` *vdc* (pour tous les contextes d'unité virtuelle pris en charge)

Méthodes d'ajout de VDC pour les unités Cisco Nexus

Utilisez la gestion de sources de configuration (Configuration Source Management) pour ajouter des unités réseau Nexus et des contextes d'unité virtuelle (VDC) à IBM Security QRadar SIEM. Il existe deux façons d'ajouter plusieurs VDC à IBM Security QRadar Risk Manager.

Vous pouvez ajouter des VDC en tant que sous-unités de l'unité Nexus ou en tant qu'unités individuelles.

Affichage des contextes d'unité virtuelle

Si des VDC sont ajoutés en tant qu'unités virtuelles, chaque VDC s'affiche comme unité dans la topologie.

Si des VDC sont ajouté en tant que sous-unité, ils ne figurent pas dans la topologie. En revanche, vous pouvez les afficher dans le moniteur de configuration.

Ajout de VDC en tant que sous-unités de votre unité Cisco Nexus

Utilisez le gestionnaire de sources de configuration (Configuration Source Manager) pour ajouter des VDC en tant que sous-unités de votre unité Cisco Nexus.

Procédure

1. Utilisez le gestionnaire de sources de configuration pour ajouter l'adresse IP admin de chaque VDC.

   Pour plus d'informations, voir «Ajout d'une unité réseau», à la page 5.
2. Utilisez le gestionnaire de sources de configuration pour obtenir les informations de configuration pour votre unité Nexus.

   Pour des informations sur l'obtention de configuration d'unité, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.
3. Activez les commandes suivantes pour l'utilisation spécifié dans les données d'identification :
   - `show vdc` (contexte admin)
   - `switchto vdc` *x*, où *x* correspond aux VDC pris en charge.

   Le moniteur de configuration (Configuration Monitor) vous permet de visualiser l'unité Nexus dans la topologie et les sous-unités VDC. Pour des informations sur la visualisation d'unités, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Ajout de VDC en tant qu'unités individuelles

Utilisez le gestionnaire de sources de configuration (Configuration Source Manager) pour ajouter chaque VDC en tant qu'unité distincte. Lorsque vous utilisez cette méthode, l'unité Nexus et les VDC figurent dans la topologie.

Lorsque vous visualisez votre unité Cisco Nexus et les VDC dans la topologie, le confinement de châssis est représenté séparément.

Procédure

1. Utilisez le gestionnaire de sources de configuration pour ajouter l'adresse IP admin de chaque VDC.

Pour plus d'informations, voir «Ajout d'une unité réseau», à la page 5.

2. Utilisez le gestionnaire de sources de configuration pour obtenir les informations de configuration pour vos VDC.
3. Sur l'unité Cisco Nexus, utilisez l'interface de ligne de commande Cisco Nexus pour désactiver la commande **switchto vdc** pour le nom d'utilisateur associé à l'adaptateur.

   Exemple : Si le nom d'utilisateur d'une unité Cisco Nexus est *qrmuser*, tapez les commandes suivantes :

```
NexusDevice(config)# role name qrmuser
NexusDevice(config-role)# rule 1 deny command switchto vdc
NexusDevice(config-role)# rule 2 permit command show
NexusDevice(config-role)# rule 2 permit command terminal
NexusDevice(config-role)# rule 2 permit command dir
```

Cisco Security Appliances

Pour intégrer IBM Security QRadar Risk Manager à vos unités réseau, veillez à vérifier les exigences relatives à l'adaptateur Cisco Security Appliances.

L'adaptateur Cisco Security Appliances collecte des configurations d'unité en sauvegardant des unités de la famille Cisco. La liste suivante fournit des exemples de pare-feu Cisco pris en charge par l'adaptateur pour Cisco Security Appliances :

- Dispositif ASA (Adaptive Security Appliance) autonome
- Module FWSM (Firewall Service Module)
- Module sur un châssis Catalyst
- Unité PIX (Private Internet Exchange) établie

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Cisco Security Appliances.

Tableau 9. Exigences d'intégration pour l'adaptateur Cisco Security Appliances

Exigence d'intégration	Description
Versions	Dispositifs ASA (Adaptive Security Appliance) utilisant un système d'exploitation Private Internet Exchange (PIX-OS) Routeurs ou commutateurs ASA utilisant FWSM Routeurs Cisco IOS série 7600 utilisant FWSM. Utilisez l'adaptateur ASA pour sauvegarder la configuration et l'état des services de carte FWSM.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à PIX ou Adaptive Security Appliance ou Firewall Service Module dans SNMP sysDescr.

Paramètres de données d'identification obligatoires	`Username`
	
	`Password`
	
	`Enable Password`

Tableau 9. Exigences d'intégration pour l'adaptateur Cisco Security Appliances (suite)

Exigence d'intégration	**Description**
Protocoles de connexion	Telnet SSH + SCP

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`change context`
	
	`change context` *`contexte-admin`*
	
	`change context` *`contexte`*
	
	`change system`
	
	`get startup-config`
	
	`show arp`
	
	`show context`
	
	`show interface`

Tableau 9. Exigences d'intégration pour l'adaptateur Cisco Security Appliances (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données (suite)	`show interface detail`
	
	`show ipv6 interface`
	
	`show ipv6 neighbor`
	
	`show mac-address-table`
	
	`show names`
	
	`show ospf neighbor`
	
	`show pager`
	
	`show route`
	
	`show running-config`
	
	`show shun`
	
	`show version`
	
	`terminal pager 0`
	
	`terminal pager 24`
	Où :
	
	La commande `show pager` doit être activer pour accéder aux comptes utilisant QRadar Risk Manager.
	
	La commande `context` *`contexte`* est utilisée pour chaque contexte sur l'unité ASA.
	
	La commande `change system` détecte si le système possède des configuration multi-contexte et détermine le contexte-admin.
	
	La commande `change context` est requise si la commande `change system` possède une configuration multi-contexte ou un contexte de configuration d'admin.
	
	Les commandes `terminal pager` sont utilisées pour définir et réinitialiser le comportement de pagination.

HP Networking ProVision

IBM Security QRadar Risk Manager prend en charge l'adaptateur HP Networking ProVision.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur HP Networking ProVision.

Tableau 10. Exigences d'intégration pour l'adaptateur HP Networking ProVision

Exigence d'intégration	**Description**
Versions	Commutateurs HP Networking ProVision K/KA.11.XX et version ultérieure. **Restriction :** Les commutateurs HP sous système d'exploitation Comware ne prennent pas en charge cet adaptateur.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond aux numéros de version au format `HP(.*)Switch(.*)(révision [A-Z]{1,2}\.(\d+)\.(\d+))` dans sysDescr.

Paramètres de données d'identification obligatoires	`Username`
	
	`Password`
	
	`Enable Password`

Protocoles de connexion	SSH

Tableau 10. Exigences d'intégration pour l'adaptateur HP Networking ProVision (suite)

Exigence d'intégration	Description

Commandes d'opération de sauvegarde émises par l'adaptateur à destination de l'unité	`dmesgshow system power-supply`
	
	`getmib`
	
	`show access-list vlan <vlan id>`
	
	`show access-list`
	
	`show access-list <name or number>`
	
	`show access-list ports <port number>`
	
	`show config`
	
	`show filter`
	
	`show filter <id>`
	
	`show running-config`
	
	`show interfaces brief`
	
	`show interfaces <interface id>` pour chaque interface.
	
	`show jumbos`
	
	`show trunks`
	
	`show lacp`
	
	`show module`
	
	`show snpm-server`
	
	`show spanning-tree`
	
	`show spanning-tree config`
	
	`show spanning-tree instance <id or list>` - pour chaque arbre maximal configuré sur l'unité
	
	`show spanning-tree mst-config`
	
	`show system information`
	
	`show version`
	
	`show vlans`
	
	`show vlans <id>` pour chaque réseau local virtuel.
	
	`show vrrp`
	
	`walkmib`

Tableau 10. Exigences d'intégration pour l'adaptateur HP Networking ProVision (suite)

Exigence d'intégration	Description

Commandes d'opération de sauvegarde `show ip` émises par l'adaptateur à destination de l'unité	`show ip`
	`show ip route`
	`show ip odpf`
	`show ip odpf redistribute`
	`show ip rip`
	`show ip rip redistribute`

Commandes de télémétrie et de données de voisinage	`getmib`
	`show arp`
	`show cdp neighbors`
	`show cdp neighbors detail <port number>`
	`show interfaces brief`
	`show interface`
	`show ip route`
	`show lldp info remote-device`
	`show lldp info remote-device <port number>`
	`show mac-address or show mac address`
	`show system information`
	`show vlans`
	`show vlans custom id state ipaddr ipmask`
	`walkmib`

Juniper Networks JUNOS

Pour intégrer IBM Security QRadar Risk Manager à vos unités réseau, veillez à vérifier les exigences relatives à l'adaptateur Juniper Networks JUNOS.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Juniper Networks JUNOS.

Tableau 11. Exigences d'intégration pour l'adaptateur Juniper Networks JUNOS

Exigence d'intégration	Description
Versions	Version 9 et ultérieures.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à SNMP sysOID: 1.3.6.1.4.1.2636
Paramètres de données d'identification obligatoires	`Username` `Password`

Tableau 11. Exigences d'intégration pour l'adaptateur Juniper Networks JUNOS (suite)

Exigence d'intégration	Description
Protocoles de connexion	Telnet SSH + SCP

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`show version`
	`show system uptime`
	`show chassis hardware`
	`show chassis firmware`
	`show chassis mac-address`
	`show chassis routing-engine`
	`show configuration snmp`
	`show snmp mib walk system configure`
	`show configuration firewall`
	`show configuration firewall family inet6`
	`show configuration security`
	`show configuration security zones`
	`show interfaces`
	`show interfaces filters`
	`show ospf interface detail`
	`show bgp neighbor`
	`show configuration routing-option`
	`show arp no-resolve`
	`show ospf neighbor`
	`show rip neighbor`
	`show bgp neighbor`
	`show ipv6 neighbors`

Juniper Networks NSM

L'adaptateur IBM Security QRadar Risk Manager prend en charge Juniper Networks NSM.

Vous pouvez utiliser QRadar Risk Manager pour sauvegarder une unité Juniper Networks unique ou pour obtenir des informations d'unité à partir d'une console Juniper Networks NSM.

La console Juniper Networks NSM contient des informations de configuration et d'unité pour les routeurs et commutateurs Juniper Networks qui sont gérés par la console Juniper Networks NSM.

Le tableau suivant décrit les environnements pris en charge pour Juniper Networks NSM.

Tableau 12. Environnements pris en charge par l'adaptateur QRadar Risk Manager pour Juniper Networks NSM

Environnement pris en charge	Description
Versions	Dispositifs IDP gérés par NSM
Prise en charge des données de voisinage	Pas de prise en charge
Reconnaissance SNMP	Pas de prise en charge
Paramètres de données d'identification obligatoires	• `Username` • `Password`
Protocoles de connexion	• SOAP • HTTP

Juniper Networks ScreenOS

Pour intégrer IBM Security QRadar Risk Manager à vos unités réseau, veillez à vérifier les exigences relatives à l'adaptateur Juniper Networks ScreenOS.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Juniper Networks ScreenOS.

Tableau 13. Exigences d'intégration pour l'adaptateur Juniper Networks ScreenOS

Exigence d'intégration	Description
Versions	Pare-feu utilisant un système d'exploitation ScreenOS
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	Correspond à netscreen ou SSG dans SNMP sysDescr.
Paramètres de données d'identification obligatoires	`Username` `Password`
Protocoles de connexion	Telnet SSH

Tableau 13. Exigences d'intégration pour l'adaptateur Juniper Networks ScreenOS (suite)

Exigence d'intégration	Description

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`set console page 0`
	`get system`
	`get config`
	`get snmp`
	`get memory`
	`get file info`
	`get file`
	`get service`
	`get group address`*`zonegroupe`*
	`get address`

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données (suite)	`get service group`
	`get service group` *`variable`*
	`get interface`
	`get interface`*`variable`*
	`get policy all`
	`get policy id`*`variable`*
	`get admin user`
	`get route`
	`get arp`
	`get mac-learn`
	`get counter statistics interface` *`variable`*
	Où :
	zone correspond aux données de zone renvoyées par la commande `get config`.
	groupe correspond aux données de groupe renvoyées par la commande `get config`.
	variable est la liste des données renvoyées à partir de la commande `get service group`, `get interface` ou `get policy id`.

Palo Alto

IBM Security QRadar Risk Manager prend en charge l'adaptateur Palo Alto. L'adaptateur Palo Alto utilise 'interface de programme d'application (API) Rest XML PAN-OS pour communiquer avec les unités.

Vous utilisez une demande HTTPS adressée à une URL pour envoyer une commande à une unité. Le format de commande pour la demande est `https://deviceIPAddress/api/?type=op&cmd=<commande>`

Où *commande* est un ensemble de balises XML ou un chemin XPath.

Exemple d'ensemble de balises XML.

```
<show><system><info></info></system></show>
```

Exemple de chemin XPath :

```
/config/predefined/service
```

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Palo Alto.

Tableau 14. Exigences d'intégration pour l'adaptateur Palo Alto

Exigence d'intégration	**Description**
Versions	PAN-OS version 4.1.0 et ultérieure.
Prise en charge des données de voisinage	Pris en charge
Reconnaissance SNMP	SysDescr correspond à 'Palo Alto Networks(.*)series firewall' ou sysOid correspond à 'panPA'

Paramètres de données d'identification obligatoires	`Username`
	
	`Password`
	
	Utilisez l'accès SuperReader pour les données d'identification.

Protocoles de connexion	HTTPS

Tableau 14. Exigences d'intégration pour l'adaptateur Palo Alto (suite)

Exigence d'intégration	Description
Commandes utilisées pour l'opération de sauvegarde	<show><system><info></info></system></show> <show><config><running></running></config></show> <show><routing><route></route></routing></show> <show><virtual-wire>all</virtual-wire></show> <show><vlan>all</vlan></show> <show><interface>all</interface></show> <show><system><disk-space></disk-space></system></show> <show><system><resources></resources></system></show> /config/predefined/service
Commandes utilisées pour la télémétrie et les données des voisinage	<show><system><info></info></system></show> <show><interface>all</interface></show> <show><routing><interface></interface></routing></show> <show><counter><interface>all</interface></counter></show> <show><arp>all</arp></show> <show><mac>all</mac></show> <show><routing><route></route></routing></show>
Commandes utilisées pour GetApplication	<show><config><running></running></config></show> /config/predefined/application

Sourcefire 3D Sensor

Pour intégrer IBM Security QRadar Risk Manager à vos unités réseau, veillez à vérifier les exigences relatives à l'adaptateur Sourcefire 3D Sensor.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Sourcefire 3D Sensor.

Limitations :

- Les règles d'intrusion associées à des règles de contrôle d'accès individuelles ne sont pas utilisées par QRM. Seule la règle d'intrusion par défaut est prise en charge.
- Lz conversion d'adresses réseau et VPN ne sont pas pris en charge.

Tableau 15. Exigences d'intégration pour l'adaptateur Sourcefire 3D Sensor

Exigence d'intégration	**Description**
Versions	5.2
Prise en charge des données de voisinage	Non
Reconnaissance SNMP	Non
Paramètres de données d'identification obligatoires	`Username` `Password`
Protocoles de connexion	SSH

Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	`show version`
	`show memory`
	`show network`
	`show interfaces`
	`expert`
	`sudo`
	`su`
	`df`
	`hostname`
	`ip addr`
	`route`
	`cat`
	`find`
	`head`
	`mysql`

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans 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 actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. 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, le logo IBM et ibm.com sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays. Si ces marques et d'autres marques d'IBM sont accompagnées d'un symbole de marque (® ou ™), ces symboles signalent des marques d'IBM aux Etats-Unis à la date de publication de ce document. Ces marques peuvent également exister et éventuellement avoir été enregistrées dans d'autres pays. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

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

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

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Remarques sur les règles de confidentialité

Les produits IBM Software, notamment les logiciels sous forme de services ("Offres logicielles"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations d'utilisation en vue d'améliorer l'expérience de l'utilisateur final, d'ajuster les interactions avec l'utilisateur final ou à d'autres fins. Dans de nombreux cas, aucune information identifiant la personne n'est collectée par les offres logicielles. Certaines de nos Offres logicielles vous permettent de collecter des informations identifiant la personne. Si cette Offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont énoncées ci-dessous.

Selon les configurations déployées, cette Offre logicielle peut utiliser des cookies de session qui collectent chaque ID de session à des fins de gestion de la session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres personnes via des cookies et d'autres technologies, vous devez vous renseigner sur l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

Pour plus d'informations sur l'utilisation de diverses technologies, notamment de cookies, à ces fins, reportez-vous aux Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et à la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site http://www.ibm.com/privacy/details/fr/fr,

ainsi qu'à la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site http://www.ibm.com/software/info/product-privacy (en anglais).

Index