

IBM Security QRadar

*Guide de configuration des
adaptateurs*

Mai 2018

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 67.

Table des matières

Avis aux lecteurs canadiens	v
Introduction à la configuration d'adaptateurs pour QRadar Risk Manager	vii
Chapitre 1. Présentation des adaptateurs	1
Types d'adaptateur	1
Fonctions des adaptateurs	2
Foire aux questions sur les adaptateurs	3
Chapitre 2. Installation des adaptateurs	7
Désinstallation d'un adaptateur	8
Chapitre 3. Méthodes d'ajout des unités réseau	9
Ajout d'une unité réseau	9
Ajout d'unités gérées par une console NSM.	11
Ajout à QRadar Risk Manager de périphériques gérés par une console CPSMS.	12
Ajout de périphériques gérés par CPSMS à l'aide d'OPSEC	13
Ajout de périphériques gérés par CPSMS à l'aide de HTTPS	14
Ajout d'unités gérées par Palo Alto Panorama	15
Palo Alto Panorama	16
Ajout d'unités gérées par SiteProtector	17
Chapitre 4. Identification et résolution des problèmes de reconnaissance et de sauvegarde de périphérique	19
Chapitre 5. Adaptateurs pris en charge	25
Brocade vRouter	26
Check Point SecurePlatform Appliances	26
Adaptateur Check Point Security Management Server	27
Adaptateur OPSEC Check Point Security Management Server	28
Adaptateur HTTPS Check Point Security Management Server	29
Cisco CatOS	31
Cisco IOS	33
Cisco Nexus	36
Méthodes d'ajout de VDC pour les unités Cisco Nexus	39
Ajout de VDC en tant que sous-unités de votre unité Cisco Nexus	39
Ajout de VDC en tant qu'unités individuelles	40
Cisco Security Appliances	40
F5 BIG-IP	43
Fortinet FortiOS	47
Adaptateur SNMP générique	48
HP Networking ProVision	50
Juniper Networks JUNOS	53
Juniper Networks NSM	55
Juniper Networks ScreenOS	56
Palo Alto	58
Sidewinder	60
Sourcefire 3D Sensor	61
Adaptateur IPS TippingPoint	64
Remarques	67
Marques	69
Dispositions relatives à la documentation du produit	69

Déclaration IBM de confidentialité en ligne. 70

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. QRadar Risk Manager utilise des adaptateurs pour s'intégrer aux unités de votre réseau.

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 à IBM Knowledge Center (<http://www.ibm.com/support/knowledgecenter/SS42VS/welcome>).

Pour plus d'informations sur la façon d'accéder à des documents plus techniques dans la bibliothèque de produits QRadar, voir *Accessing IBM Security QRadar Documentation* (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contactez le service clients

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

Instructions relatives aux bonnes pratiques de sécurité

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

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi

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

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).

Topologie de réseau et configuration

QRadar Risk Manager utilise des adaptateurs pour collecter des configurations de réseau. Les adaptateurs transforment les informations de configuration en un format standard 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 au réseau, QRadar Risk Manager doit pouvoir accéder aux unités. QRadar Risk Manager utilise les données d'identification utilisateur qui sont configurées dans QRadar pour accéder à l'unité et recevoir par téléchargement les configurations.

Processus d'intégration d'unités réseau

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

1. Configurez le périphérique réseau pour permettre la communication avec QRadar Risk Manager.
2. Installez l'adaptateur approprié à votre unité réseau sur votre dispositif QRadar Risk Manager.
3. Utilisez Configuration Source Management pour ajouter vos unités réseau à QRadar Risk Manager.
4. Définissez le protocole de réseau qui est requis pour la communication avec vos périphériques réseau.

Pour plus d'informations, voir 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 :

- F5 BIG-IP
- Brocade vRouter
- Check Point SecurePlatform Appliances
- Check Point Security Management Server
- Cisco Catalyst (CatOS)
- Cisco Internet Operating System (IOS)
- Cisco Nexus
- Cisco Security Appliances
- Fortinet FortiOS
- HP Networking ProVision

- Juniper Networks ScreenOS
- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto
- Sourcefire 3D Sensor
- SNMP générique
- IPS TippingPoint
- McAfee Sidewinder

Fonctions des adaptateurs

Les adaptateurs sont fournis avec de nombreuses fonctions qui vous aident à intégrer vos périphériques réseau à QRadar Risk Manager.

Le tableau suivant répertorie les fonctions communes des adaptateurs pris en charge.

Tableau 1. Fonctions des adaptateurs

Adaptateur	Versions	NAT	Routing	Tunnellisation	Protocoles	Autres fonctions
Brocade vRouter	6.7 à 17.1		Statique		Telnet, SSH	
Check Point Secure Platform	R65 à R77.30	Statique Dynamique	Statique		Telnet, SSH	
Check Point SMS OPSEC	NGX R60 à R77	Statique Dynamique	Statique		CPSMS	
Check Point SMS HTTPS	R80	Statique Dynamique	Statique		HTTPS	
Cisco ASA	ASA : 8.2, 8.4 à 9.1.7 PIX : 6.1, 6.3 FWSM : 3.1, 3.2	Statique	Statique EIGRP, OSPF		Telnet, SSH, SCP	
Cisco CatOS	Catalyst série 6500 - périphériques châssis. 4.2, 6.4		Statique		Telnet, SSH	
Cisco Nexus	Nexus 5548 : système d'exploitation niveau 6.0 Nexus 7000 series : système d'exploitation niveau 6.2 Nexus 9000 series : système d'exploitation niveau 6.1		Statique EIGRP, OSPF		Telnet, SSH	
Cisco IOS	IOS 12.0 à 15.1 pour les routeurs et les commutateurs Commutateurs Cisco Catalyst 6500 avec MSFC.	Statique Dynamique	Statique EIGRP, OSPF	VPN	Telnet, SSH	

Tableau 1. Fonctions des adaptateurs (suite)

Adaptateur	Versions	NAT	Routage	Tunnellisation	Protocoles	Autres fonctions
F5 BIG-IP	10.1.1, 11.4.1	Statique Dynamique	Statique	VPN	SSH	
Fortinet FortiOS	Versions 4.0 MR3 à 5.2.4	Statique	Statique		Telnet, SSH	
SNMP générique	SNMPv1, v2 et v3					
HP ProCurve ProVision	HP Networking ProVision Switches K/KA.15.X		RIP		SSH	
IBM Proventia GX IPS	Dispositifs GX gérés par SiteProtector.				SQL	Applications
Juniper JUNOS	10.4, 11.2 à 12.3 et 13.2	Statique Dynamique	Statique OSPF		Telnet, SSH, SCP	
Juniper NSM	Dispositifs IDP gérés par NSM				HTTPS	
Juniper ScreenOS	5.4, 6.2	Statique Dynamique	Statique		Telnet, SSH	
Sidewinder	8.3.2	Statique	Statique		Telnet, SSH	
Pare-feux Palo Alto	Versions PAN-OS 5.0 à 7.0	Statique Dynamique	Statique	IPSEC	HTTPS	Utilisateur/ Groupes Applications
SourceFire 3D Sensor	5.3			VPN	SSH	IPS
IPS TippingPoint	TOS 3.6 et SMS 4.2				Telnet, SSH, HTTPS	IPS

Foire aux questions sur les adaptateurs

QRadar Risk Manager utilise des adaptateurs pour se connecter et obtenir des périphérique réseau des informations de configuration.

Les adaptateurs prennent-ils en charge tous les périphériques et versions que QRadar SIEM prend en charge ?

Les adaptateurs sont une intégration distincte et QRadar Risk Manager ne les utilise que pour importer des configurations de périphérique. Pour afficher la liste des adaptateurs pris en charge, voir Chapitre 5, «Adaptateurs pris en charge», à la page 25.

Tous les adaptateurs prennent-ils en charge les mêmes fonctions, par exemple, le routage OSPF ?

La gamme des fonctions prises en charge tels le routage et NAT varie selon les adaptateurs. Voir «Fonctions des adaptateurs», à la page 2.

Quel niveau d'accès utilisateur est nécessaire à l'adaptateur pour obtenir une configuration de périphérique ?

Le niveau d'accès utilisateur requis varie en fonction de l'adaptateur mais il est limité à la lecture seule pour la plupart des adaptateurs. Voir la rubrique Chapitre 5, «Adaptateurs pris en charge», à la page 25 et affichez les exigences de niveau d'accès utilisateur lorsque vous sélectionnez un adaptateur.

Comment configurer les données d'identification pour accéder à aux périphériques réseau ?

Vous devez configurer les données d'identification de manière à autoriser QRadar Risk Manager à se connecter aux périphériques de votre réseau. Les administrateurs utilisent Configuration Source Management pour entrer les données d'identification de périphérique. Les données de périphérique individuelles peuvent être sauvegardées pour un périphérique de réseau spécifique. Si plusieurs périphériques réseau utilisent les mêmes données d'identification, vous pouvez affecter ces données à un groupe. Pour plus d'informations, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Quelles zones de données d'identification doivent être renseignées pour chaque périphérique ?

Certains adaptateurs peuvent ne nécessiter qu'un nom d'utilisateur et un mot de passe tandis que d'autres requièrent des données d'identification supplémentaires, par exemple, Cisco IOS peut exiger un mot de passe d'activation. Voir Chapitre 5, «Adaptateurs pris en charge», à la page 25 et affichez les paramètres de données d'identification requis dans les tables.

Comment configurer les protocoles pour les périphériques ?

Utilisez des groupes réseau, qui contiennent les protocoles utilisables pour activer la connectivité aux plages d'adresses IP/CIDR/ pour les périphériques. Pour plus d'informations, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Comment ajouter les périphériques réseau dans QRadar Risk Manager ?

Le Tableau 1 répertorie les méthodes d'ajout de périphériques réseau dans QRadar Risk Manager.

Tableau 2. Ajout de périphériques réseau

Méthode	Description
Ajout de périphériques individuellement	Utilisez cette méthode si vous voulez effectuer une sauvegarde de test de quelques périphériques, par exemple, pour vérifier si vos données d'identification et protocoles sont correctement configurés.
Reconnaissance de périphérique	Utilisez cette méthode si vous avez une plage d'adresses IP/CIDR avec des noms de communauté SNMP configurés pour chaque périphérique et que vous voulez rechercher tous les périphériques dans cette plage d'adresses. Les noms de communauté SNMP doivent être définis dans votre ensemble de données d'identification pour que la reconnaissance de périphérique fonctionne.
Reconnaissance à partir d'un périphérique de gestion	Utilisez cette méthode pour les périphériques gérés par un système de gestion pris en charge tel que Check Point SMS.
Importation de périphériques	Si votre réseau contient plusieurs périphériques, cette méthode est la plus fiable.

Pour plus d'informations sur l'ajout de périphériques réseau dans QRadar Risk Manager, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Chapitre 2. Installation des adaptateurs

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

Avant de commencer

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 tant qu'utilisateur root.
2. Téléchargez le fichier compressé destiné aux adaptateurs QRadar Risk Manager depuis Fix Central (www.ibm.com/support/fixcentral/) vers votre console QRadar SIEM Console.
3. Pour copier le fichier compressé depuis votre console QRadar SIEM Console dans QRadar Risk Manager, tapez la commande suivante :

```
scp adaptateurs.zip root@adresse_IP :
```

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

Exemple :

```
scp adapters.bundle-2014-10-972165.zip 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. Pour extraire et installer les adaptateurs, tapez les commandes suivantes depuis le répertoire principal contenant le fichier compressé :

```
unzip adaptateurs.zip
```

```
yum install -y adapters*.rpm
```

Exemple :

```
unzip adapters.bundle-2014-10-972165.zip
```

```
yum install -y adapters*.rpm
```

Remarque :

Pour les versions de QRadar Risk Manager antérieures à 7.2.8, utilisez la commande **rpm**.

Exemple :

```
rpm -Uvh adapters*.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 Configuration Source Management.

Désinstallation d'un adaptateur

Utilisez la commande **yum** 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 tant qu'utilisateur root.
2. Pour désinstaller un adaptateur, tapez la commande suivante :

```
yum remove -y package_adaptateur
```

Par exemple, `yum remove -y adapters.cisco.ios-2011_05-205181.noarch`

Remarque :

Pour les versions de QRadar Risk Manager antérieures à 7.2.8, utilisez la commande **rpm**.

Exemple :

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

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

Chapitre 3. Méthodes d'ajout des unités réseau

Utilisez 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 3. Méthodes d'ajout d'une unité réseau à QRadar Risk Manager

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


Ajout d'une unité réseau

Pour ajouter une unité réseau à IBM Security QRadar Risk Manager, utilisez 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 5, «Adaptateurs pris en charge», à la page 25.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins** ou sur **Applications**.
 - Dans IBM Security QRadar V7.3.0 ou version antérieure, cliquez sur **Plug-ins**.
 - Dans IBM Security QRadar V7.3.1, cliquez sur **Applications**.
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. Entrez le nom du groupe de réseau et cliquez sur **OK**.
 - b. Entrez l'adresse IP de votre périphérique, puis cliquez sur **Add**.

Vous pouvez entrer une adresse IP, une plage d'adresses IP, un sous-réseau CIDR ou un caractère générique.

Par exemple, utilisez format suivant pour un caractère générique, 10.1.*.*

Par exemple, utilisez le format suivant pour un CIDR, 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**, à côté de 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. Entrez le nom de 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 4. 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 Configuration Source Management :

- 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.

Pour plus d'informations sur la configuration des sources, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.

7. Dans le menu de navigation, ajoutez une ou plusieurs unités.
 - Pour ajouter une unité réseau, cliquez sur **Add Device**.
 - Pour ajouter plusieurs adresses IP pour des unités réseau, cliquez sur **Discover Devices**.
8. Entrez l'adresse IP de l'unité, sélectionnez le type d'adaptateur, puis cliquez sur **Add**.
Si l'unité n'est pas sauvegardée, un point d'interrogation bleu s'affiche en regard de l'adaptateur.
9. Pour sauvegarder l'unité que vous ajoutez à la liste des unités, sélectionnez-la, puis cliquez sur **Save**.
10. Répétez cette procédure pour chaque unité réseau à ajouter à la liste.

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 NSM

Utilisez Configuration Source Management pour ajouter toutes les unités provenant d'une console Juniper Networks NSM à IBM Security QRadar Risk Manager.

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 5, «Adaptateurs pris en charge», à la page 25.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins** ou sur **Applications**.
 - Dans IBM Security QRadar V7.3.0 ou version antérieure, cliquez sur **Plug-ins**.
 - Dans IBM Security QRadar V7.3.1, cliquez sur **Applications**.
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. Entrez le nom du groupe de réseau et cliquez sur **OK**.
 - b. Entrez l'adresse IP de votre périphérique, puis cliquez sur **Add**.
Vous pouvez entrer une adresse IP, une plage d'adresses IP, un sous-réseau CIDR ou un caractère générique.

- 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**, à côté de 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. Entrez le nom de 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 5. 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 (Network and Security Manager) ne prend pas en charge 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 sur **GO**.
 9. Sélectionnez l'unité que vous venez d'ajouter à la liste des unités, 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, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Ajout à QRadar Risk Manager de périphériques gérés par une console CPSMS

Utilisez Configuration Source Management pour ajouter des périphériques à IBM Security QRadar Risk Manager depuis un serveur CPSMS (Check Point Security Manager Server).

En fonction de votre version de Check Point Security Manager Server, vous devez choisir l'une des méthodes de reconnaissance suivantes pour ajouter vos périphériques à QRadar Risk Manager.

Ajout de périphériques gérés par CPSMS à l'aide d'OPSEC

Ajoutez des périphériques gérés par Check Point Security Manager Server versions NGX R60 à R77 à IBM Security QRadar Risk Manager en utilisant OPSEC pour les reconnaître et les ajouter.

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 5, «Adaptateurs pris en charge», à la page 25.


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* avant de débiter cette procédure. Pour plus d'informations, reportez-vous à votre documentation CPSMS.

Remarque : La fonction d'importation d'unité n'est pas compatible avec les adaptateurs CPSMS.

Pourquoi et quand exécuter cette tâche

Effectuez la procédure suivante pour chaque unité CPSMS à laquelle vous voulez vous connecter, et pour lancer la reconnaissance de ses pare-feux gérés.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le menu de navigation **Admin**, cliquez sur **Applications**.
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. Entrez le nom du groupe de réseau et cliquez sur **OK**.
 - b. Entrez l'adresse IP de votre périphérique 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**, à côté de la zone **Add address**.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
 - a. Entrez le nom de 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. Cette valeur doit être exacte car le format dépend du type d'unité d'où provient la reconnaissance. Utilisez le tableau ci-dessous comme référence aux formats de nom OPSEC Entity SIC.

Type	Nom
Serveur de gestion	CN=cp_mgmt,0=<take 0 value from DN field>
Passerelle vers un serveur de gestion	CN=cp_mgmt_<gateway hostname>,0=<take 0 value from DN field>

Par exemple, vous effectuez une reconnaissance depuis un serveur de gestion :

- DN de l'application OPSEC: CN=cpsms226,0=vm226-CPSMS..bs7ocx
- Hôte de l'application OPSEC : vm226-CPSMS

Le nom de l'entité Entity SIC est CN=cp_mgmt,0=vm226-CPSMS..bs7ocx

Si vous effectuez une reconnaissance depuis la passerelle vers un serveur de gestion :

- DN de l'application OPSEC : CN=cpsms230,0=vm226-CPSMS..bs7ocx
- Hôte de l'application OPSEC : vm230-CPSMS2-GW3

Le nom de l'entité Entity SIC est CN=cp_mgmt_vm230-CPSMS2-GW3,0=vm226-CPSMS..bs7ocx

8. Utilisez l'application Check Point SmartDashboard pour entrer le nom OPSEC Application Object SIC, qui a été créé sur le serveur CPSMS.
Exemple : CN=cpsms230,0=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 **Protocols** et vérifiez que le protocole **CPSMS** est sélectionné.
Le port par défaut du protocole CPSMS est 18190.
12. Cliquez sur **Discover From Check Point OPSEC**, puis entrez l'adresse IP de CPSMS.
13. Cliquez sur **OK**.
14. Répétez cette procédure pour chaque périphérique CPSMS à ajouter.


Que faire ensuite

Après avoir ajouté tous les périphériques requis, sauvegardez-les puis affichez-les dans la topologie.

Ajout de périphériques gérés par CPSMS à l'aide de HTTPS

Ajoutez des périphériques gérés par Check Point Security Manager Server version R80 à IBM Security QRadar Risk Manager en utilisant le protocole HTTPS pour les reconnaître et les ajouter.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins** ou sur **Applications**.
 - Dans IBM Security QRadar V7.3.0 ou version antérieure, cliquez sur **Plug-ins**.
 - Dans IBM Security QRadar V7.3.1, cliquez sur **Applications**.
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. Entrez le nom du groupe de réseau et cliquez sur **OK**.
 - b. Entrez l'adresse IP de votre périphérique Check Point, puis cliquez sur **Add**.
 - c. Assurez-vous que l'adresse s'affiche dans la zone **Network address**.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
 - a. Entrez le nom de 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. Cliquez sur **OK**.
8. Cliquez sur **Protocols** et vérifiez que le protocole **HTTPS** est sélectionné.
9. Cliquez sur **Discover From Check Point HTTPS**, puis entrez l'adresse IP de Check Point.
10. Cliquez sur **OK**.


Que faire ensuite

Après avoir ajouté tous les périphériques requis, sauvegardez-les puis affichez-les dans la topologie.

Ajout d'unités gérées par Palo Alto Panorama

Utilisez Configuration Source Management pour ajouter à IBM Security QRadar Risk Manager des unités provenant de Palo Alto Panorama.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins** ou sur **Applications**.
 - Dans IBM Security QRadar V7.3.0 ou version antérieure, cliquez sur **Plug-ins**.
 - Dans IBM Security QRadar V7.3.1, cliquez sur **Applications**.
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. Entrez le nom du groupe de réseau et cliquez sur **OK**.
 - b. Entrez l'adresse IP de votre unité Palo Alto Panorama puis cliquez sur **Add**.
 - c. Assurez-vous que les adresses que vous ajoutez s'affichent dans la zone **Network address**, à côté de la zone **Add address**.
Palo Alto Panorama prend en charge les sauvegardes de proxy.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
 - a. Indiquez le nom de l'ensemble de données d'identification puis 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. Cliquez sur **OK**.

8. Cliquez sur **Discover From Palo Alto Panorama** puis entrez l'adresse IP de Palo Alto Panorama.
Palo Alto Panorama utilise la commande suivante pour la sauvegarde :
`api/?type=op&cmd=<show><devices><connected></connected></devices></show>`
9. Cliquez sur **OK**.

Que faire ensuite

Après avoir ajouté tous les périphériques requis, sauvegardez-les puis affichez-les dans la topologie.

Palo Alto Panorama

IBM Security QRadar Risk Manager prend en charge le serveur de gestion de sécurité Palo Alto Panorama.

Palo Alto Panorama prend en charge les sauvegardes de proxy.

Les sauvegardes des unités reconnues par le serveur de gestion de sécurité réseau Palo Alto Panorama sont collectées à partir de l'emplacement Panorama où elles sont effectuées.

Le tableau suivant présente les exigences d'intégration pour Palo Alto Panorama.

Tableau 6. Exigences d'intégration pour Palo Alto Panorama

Exigence d'intégration	Description
Versions	8.0
Niveau d'accès utilisateur minimum	Accès superutilisateur (accès complet) requis pour les unités PA qui comportent des listes de blocs dynamiques pour exécuter des commandes de niveau système. Accès superutilisateur (en lecture seule) pour toutes les autres unités PA.
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	HTTPS
Commandes devant être utilisées pour l'opération de sauvegarde.	<code>api/?type=op&cmd=<show><devices><connected></connected></devices></show></code>

Ajout d'unités gérées par SiteProtector


Utilisez Configuration Source Management pour ajouter des unités de 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. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le menu de navigation **Admin**, cliquez sur **Plug-ins** ou sur **Applications**.
 - Dans IBM Security QRadar V7.3.0 ou version antérieure, cliquez sur **Plug-ins**.
 - Dans IBM Security QRadar V7.3.1, cliquez sur **Applications**.
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. Entrez le nom du groupe de réseau et cliquez sur **OK**.
 - b. Entrez l'adresse IP de votre périphérique SiteProtector, puis cliquez sur **Add**.
 - c. Assurez-vous que les adresses que vous ajoutez s'affichent dans la zone **Network address**, à côté de la zone **Add address**.
6. Dans le volet Credentials, cliquez sur **Add a new credential set**.
 - a. Indiquez le nom de 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 l'option **Discover From SiteProtector**, puis entrez l'adresse IP SiteProtector.
9. Cliquez sur **OK**.

Que faire ensuite

Après avoir ajouté tous les périphériques requis, sauvegardez-les puis affichez-les dans la topologie.

Chapitre 4. Identification et résolution des problèmes de reconnaissance et de sauvegarde de périphérique

Corrigez les anomalies liées à la reconnaissance et à la sauvegarde de périphérique. Vous pouvez consulter les détails des journaux et des messages d'erreur et d'avertissement pour vous aider à identifier et résoudre les problèmes.

Echec de sauvegarde du périphérique

Vérifiez les données d'identification pour la connexion au périphérique.

1. Dans l'onglet **Admin**, cliquez sur **Configuration Source Management**.
2. Vérifiez que les données d'identification permettant d'accéder au périphérique cible sont corrects.
3. Testez les données d'identification sur le périphérique cible.

Affichage des erreurs de sauvegarde de périphérique.

Pour afficher les erreurs de sauvegarde, procédez comme suit :

1. Dans l'onglet **Admin**, cliquez sur **Configuration Source Management**.
2. Cliquez sur un périphérique, puis sur **View error** (afficher l'erreur).

Le tableau suivant répertorie les ID message d'erreur, les descriptions de message et les actions d'identification et de résolution des problèmes suggérées.

Tableau 7. Erreurs de sauvegarde de périphérique

Erreurs de sauvegarde	Description de l'erreur	Etape d'identification et de résolution de problème suggérée
UNEXPECTED_RESPONSE	La tentative de connexion a dépassé le délai d'attente	Vérifiez que vous utilisez l'adaptateur approprié
INVALID_CREDENTIALS	Données d'identification incorrectes	Vérifiez les données d'identification dans Configuration Source Management .
SSH_ERROR	Erreur de connexion	Vérifiez que le périphérique fonctionne et est connecté à votre réseau. Utilisez d'autres protocoles de connexion réseau et des outils d'identification et de résolution de problèmes afin de vérifier que le périphérique est accessible. Vérifiez que le protocole de connexion SSH est autorisé et qu'il est correctement configuré.

Tableau 7. Erreurs de sauvegarde de périphérique (suite)

Erreurs de sauvegarde	Description de l'erreur	Etape d'identification et de résolution de problème suggérée
TELNET_ERROR	Erreur de connexion	Vérifiez que le périphérique fonctionne et est connecté à votre réseau. Utilisez d'autres protocoles de connexion réseau et des outils d'identification et de résolution de problèmes afin de vérifier que le périphérique est accessible. Vérifiez que le protocole de connexion Telnet est autorisé et qu'il est correctement configuré.
SNMP_ERROR	Erreur de connexion	Vérifiez que le périphérique fonctionne et est connecté à votre réseau. Utilisez d'autres protocoles de connexion réseau et des outils d'identification et de résolution de problèmes afin de vérifier que le périphérique est accessible. Vérifiez que le protocole SNMP est autorisé et qu'il est correctement configuré.
TOO_MANY_USERS	Le nombre d'utilisateurs configuré pour l'accès à ce périphérique est dépassé.	Vérifiez le nombre maximal d'utilisateurs autorisés à accéder à l'unité par connexion au périphérique, ainsi que la configuration du nombre maximal d'accès simultanés d'utilisateurs.
DEVICE_MEMORY_ERROR	Erreurs de configuration d'unité	Vérifiez que le périphérique fonctionne correctement. Accédez à l'unité et vérifiez la configuration, ainsi que les journaux d'erreurs. Utilisez la documentation de votre périphérique pour vous aider à identifier et résoudre les erreurs.
NVRAM_CORRUPTION_ERROR	Incidents d'accès au périphérique	Dans Configuration Source Management , vérifiez le niveau d'accès de l'utilisateur configuré pour accéder au périphérique.
INSUFFICIENT_PRIVILEGE	L'utilisateur configuré pour accéder au périphérique ne dispose pas de droits suffisants	Dans Configuration Source Management , vérifiez le niveau d'accès de l'utilisateur configuré pour accéder au périphérique.
DEVICE_ISSUE	Erreur sur l'unité	Sélectionnez le périphérique dans Configuration Source Management et cliquez sur View error (afficher l'erreur) pour plus de détails.

La sauvegarde se termine avec un avertissement d'analyse

Pour afficher plus de détails sur l'avertissement, procédez comme suit :

1. Cliquez sur l'onglet **Risks**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor** (moniteur de configuration).
3. Cliquez sur l'option de **consultation du journal** pour l'unité sélectionnée dans la table de **liste des périphériques**.

Vérifiez que vous disposez des dernières versions d'adaptateur

Pour vérifier les versions de vos adaptateurs, connectez-vous en tant qu'utilisateur root au dispositif QRadar Risk Manager puis entrez la commande suivante :

```
yum list adapter\*
```

Vous pouvez rechercher des informations de date dans les noms des adaptateurs afin de vous aider à déterminer les dates d'édition.

Pour télécharger l'ensemble d'adaptateurs le plus récent, procédez comme suit :

1. Accédez à IBM Fix Central (<https://www.ibm.com/support/fixcentral/>).
2. Dans la zone du **sélecteur de produit**, tapez Risk Manager pour filtrer votre sélection.
3. Cliquez sur IBM Security QRadar Risk Manager.
4. Depuis la liste **Version installée**, sélectionnez la version installée sur votre système.
5. Dans la liste **Plateforme**, sélectionnez le système d'exploitation installé sur votre système, puis cliquez sur **Continuer**.
6. Cliquez sur **Rechercher des correctifs** puis cliquez sur **Continuer**.
7. Pour télécharger l'ensemble d'adaptateurs le plus récent, cliquez sur le lien de l'ensemble d'adaptateurs en haut de la liste **Adaptateur**.

Vérifiez que votre sauvegarde de périphérique est la plus récente

Pour vérifier si vous disposez d'une sauvegarde récente, procédez comme suit :

1. Cliquez sur l'onglet relatif aux **risques**.
2. Dans le menu de navigation, cliquez sur l'option de **moniteur de configuration**.
3. Cliquez deux fois sur le périphérique dans la table de **liste des périphériques**.
4. Dans la barre d'outils, cliquez sur l'icône d'**historique**. La configuration importée la plus récente s'affiche.

Si vous pensez ne pas disposer de la configuration la plus récente, vérifiez-le en exécutant une nouvelle fois la sauvegarde.

Erreur lors de l'importation de configurations depuis vos périphériques

Un fichier CSV incorrectement formaté peut provoquer l'échec de la sauvegarde d'un périphérique. Exécutez la procédure suivante pour vérifier le fichier CSV :

1. Examinez votre fichier CSV pour corriger toute erreur éventuelle.

2. Réimportez votre configuration d'unité en utilisant le fichier CSV mis à jour.

Echec de la reconnaissance d'unité avec Check Point SMS (OPSEC)

Suivez la procédure complète de la section "Ajout d'unités gérées par une console CPSMS" du manuel *IBM Security QRadar Risk Manager Adapter - Guide de configuration*, notamment les étapes 7 et 8 dans lesquelles les zones OPSEC doivent être précises.

Echec de sauvegarde de périphérique en raison d'une invite de connexion ou du message du jour

Les adaptateurs qui font appel à Telnet et SSH pour se connecter à des périphériques utilisent des expressions régulières pour la mise en correspondance avec les invites de périphérique. Si des caractères de l'invite de connexion ou du message du jour correspondent à l'expression régulière, le processus de sauvegarde risque d'échouer.

Par exemple, si vous utilisez la bannière de connexion suivante pour Cisco ASA, le processus de sauvegarde échoue car l'adaptateur fonctionne comme si le caractère # de l'invite de connexion était l'invite du périphérique lorsque l'expression régulière #\s*\$ est mise en correspondance.

```
##### Welcome to ASA #####
```

Le tableau suivant répertorie les adaptateurs et leurs expressions régulières concernés par ces échecs de sauvegarde :

Tableau 8. Adaptateurs et leurs expressions régulières

Adaptateur	Expressions régulières (des guillemets simples (!) sont utilisés comme délimiteurs)
CheckPoint SecurePlatform	'sername: (?<!Last)\s+login:' '[Pp]assword:' '(# \\$ >)\s*\$'
Cisco SecurityAppliance (ASA)	'sername: ogin:' '[Pp]assword:' '>\s*\$' '#\s*\$'
Cisco Nexus	'sername:\s*' 'assword:\s*' '(^ \n \r)[^#\n\r]+\s*\$ [^#\n\r]+\s*\S+#\s*\$' '\hello>\W+?'
Cisco IOS	'maximum number of telnet' 'assword required, but none se' 'sername:' 'assword:' 'PASSCODE:' '(?m)^\w\S*#\s*(?![\n\r])\$' '(?m)^\w\S*>\s*(?![\n\r])\$' 'any key to' 'User Interface Menu'
Cisco CatOS	'sername: ogin:' '[Pp]assword:' '\n\S+\s\$' '\(enable)\s*\$' '(^ \n \r)[^>^\n\r]+>\s*\$'

Tableau 8. Adaptateurs et leurs expressions régulières (suite)

Adaptateur	Expressions régulières (des guillemets simples (')) sont utilisés comme délimiteurs)
HP ProVision	'\S+>' '\S+#' 'sername:\s*\Z' 'ogin as:'
IPS TippingPoint	'sername: ogin:' 'assword:' '(# \\$ >)\s*\$'
CheckPoint OPSEC	'sername: (?<!Last)\s+login:' '[Pp]assword:' '(# \\$ >)\s*\$'
McAfee Sidewinder	'sername: (?<!Last)\s+login: (login:\s+)\$' '[Pp]assword:' '(# \\$ > %)\s*\$'
Juniper ScreenOS	'sername: ogin:' '[Pp]assword:' '(# >)\s*\$'
Juniper JUNOS	'^\s*login:' 'assword' '%' '\.+>'
Juniper NSM	'sername: (?<!Last)\s+login:' '[Pp]assword:' '(# \\$ >)\s*\$'
Sourcefire 3D	'(# \\$ >)\s*\$' '(\>\s*expert\ a?)\s*\$' '([Pp]assword)\s*:\s*\$'
F5 BIG-IP	'sername: ogin:\s*\$' 'continue connecting \ (yes\ /no\)\ ?\s*\$' '[Pp]assword:\s*\$' '(# \\$)\s*\$'
Fortinet FortiOS	'sername: (?<!Last)\s+login:' '[Pp]assword:' '(# \\$ >)\s*\$'
Nokia CheckPoint	'sername:\s*\$ ogin:\s*\$' '[Pp]assword:' 'Terminal\s+type\ ?' '(# \\$ >)\s*\$'

Tâches associées:

«Ajout de périphériques gérés par CPSMS à l'aide d'OPSEC», à la page 13
Ajoutez des périphériques gérés par Check Point Security Manager Server versions NGX R60 à R77 à IBM Security QRadar Risk Manager en utilisant OPSEC pour les reconnaître et les ajouter.

Chapitre 5. Adaptateurs pris en charge

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

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 doivent prendre en charge MIB-2 standard pour que la reconnaissance SNMP puisse avoir lieu, et la configuration SNMP de l'unité doit être correctement prise en charge et configurée.

Paramètres de données d'identification obligatoires

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

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.

Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez **Configuration Source Management** sous l'onglet **Admin**.

Protocoles de connexion

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

Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez **Configuration Source Management** sous l'onglet **Admin**.

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.

Brocade vRouter

IBM Security QRadar Risk Manager prend en charge l'adaptateur Brocade Virtual Router (vRouter).

La fonction de routage statique est disponible avec l'adaptateur Brocade vRouter.

Les exigences d'intégration pour l'adaptateur Brocade vRouter sont présentées dans le tableau suivant :

Tableau 9. Adaptateur Brocade vRouter

Exigence d'intégration	Description
Versions prises en charge	6.7 à 17.1
Niveau d'accès utilisateur minimum	Opérateur ou Admin
Paramètres de données d'identification obligatoires	Username Password
Protocoles de connexion pris en charge	Utilisez un des protocoles de connexion pris en charge suivants : SSH Telnet
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	show version show host name show system memory show configuration all no-more show interfaces no-more

Check Point SecurePlatform Appliances

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

Les fonctions ci-dessous sont disponibles avec l'adaptateur Check Point SecurePlatform Appliances :

- Conversion d'adresses réseau (NAT) dynamique
- Conversion d'adresses réseau statique (NAT) statique
- Reconnaissance SNMP
- Routage statique
- Protocoles de connexion Telnet et SSH

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

Tableau 10. Exigences d'intégration pour l'adaptateur Check Point SecurePlatform Appliances

Exigence d'intégration	Description
Versions	R65 vers R77.30 Restriction : Les dispositifs Nokia IPSO ne sont pas pris en charge pour la sauvegarde.
Reconnaissance SNMP	Correspond à NGX dans SNMP sysDescr.
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password Enable Password (mode expert)
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Utilisez un des protocoles de connexion pris en charge suivants : Telnet SSH
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	hostname dmi decode 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

Utilisez l'adaptateur Check Point pour reconnaître et sauvegarder les noeuds d'extrémité gérés par Security Management Server (CPSMS).

Sélectionnez l'un des adaptateurs suivants pour reconnaître et sauvegarder les noeuds d'extrémité gérés par le serveur CPSMS.

Adaptateur OPSEC Check Point Security Management Server

Utilisez l'adaptateur OPSEC Check Point Security Management Server pour reconnaître et sauvegarder les noeuds d'extrémité gérés par CPSMS versions NGX R60 à R77.

Les fonctions ci-dessous sont disponibles avec l'adaptateur OPSEC Check Point Security Management Server :

- Protocole OPSEC
- Conversion d'adresses réseau (NAT) dynamique
- Conversion d'adresses réseau statique (NAT) statique
- Routage statique

L'adaptateur CPSMS est construits sur le logiciel SDK OPSEC SDK 6.0, lequel prend en charge les produits Check Point configurés pour utiliser des certificats signés avec SHA-1 uniquement.

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

Tableau 11. Exigences d'intégration pour l'adaptateur CPSMS

Exigence d'intégration	Description
Versions	NGX R60 à R77
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Utilisez les données d'identification qui sont définies à la section 'Ajout d'unités gérées par une console CPSMS'.
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	CPSMS
Exigences de configuration	Pour autoriser le client cpsms_client à communiquer avec Check Point Management Server, le fichier \$CPDIR/conf/sic_policy.conf sur CPSMS doit inclure la ligne suivante : # OPSEC applications defaultANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp# sam proxyANY ; Modules, DN_Mgmt ; ANY; sam ; sslcaANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_compANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_compANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp

Tableau 11. Exigences d'intégration pour l'adaptateur CPSMS (suite)

Exigence d'intégration	Description
Ports requis	<p>Les ports ci-dessous sont utilisés par QRadar Risk Manager et doivent être ouverts dans CPSMS :</p> <p>Port 18190 pour le service Check Point Management Interface (CPMI)</p> <p>Port 18210 pour le service Check Point Internal CA Pull Certificate Service (FW1_ica_pull)</p> <p>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, <code>cpmi_server_auth_port 18190</code>.</p>

Adaptateur HTTPS Check Point Security Management Server

Utilisez l'adaptateur HTTPS Check Point Security Management Server pour reconnaître et sauvegarder les noeuds d'extrémité connectés à des lames pare-feu qui sont gérées par Security Management Server version R80.

Les fonctions ci-dessous sont disponibles avec l'adaptateur HTTPS Check Point Security Management Server :

- Conversion d'adresses réseau statique (NAT) statique
- Routage statique
- Protocole de connexion HTTPS

Les fonctions ci-dessous ne sont pas prises en charge par l'adaptateur Check Point Security Management Server :

- Objets dynamiques (objets réseau)
- Zones de sécurité (objets réseau)
- Objets RPC (services)
- Objets DCE-RPC (services)
- Objets ICMP (services)
- Objets GTP (services)
- Objets TCP composés (services)
- Objets TCP Citrix (services)
- Autres services (services)
- Objets utilisateur
- Objets temporels
- Négation des critères de règle de contrôle d'accès

Remarque :

Si vous réalisez une mise à niveau vers Check Point Security Management Server R80 à partir d'une version antérieure de Check Point SMS, vous devez lancer une nouvelle reconnaissance des unités par la méthode de reconnaissance **Discover From Check Point HTTPS**, même si elles sont enregistrées par **Configuration Source Management**.

Le tableau suivant décrit les exigences d'intégration pour l'adaptateur Check Point Security Management Server.

Tableau 12. Exigences d'intégration pour l'adaptateur Check Point Security Management Server

Exigence d'intégration	Description
Versions	R80
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p> <p>Remarque : Vous devez entrer les données d'identification Check Point Security Management Server avant de configurer la reconnaissance de périphérique.</p>	<p>Username</p> <p>Password</p>
<p>Configuration de la reconnaissance de périphérique</p> <p>Pour configurer la reconnaissance de périphérique dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p> <p>Pour configurer la méthode de reconnaissance, cliquez sur Discover From Check Point HTTPS, entrez l'adresse IP de Check Point Security Management Server et cliquez sur OK.</p>	Discover From Check Point HTTPS
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	HTTPS
Exigences de niveau d'accès utilisateur	Read-write access all

Tableau 12. Exigences d'intégration pour l'adaptateur Check Point Security Management Server (suite)

Exigence d'intégration	Description
Noeuds finaux d'API requis	<p>Utilisez le format suivant pour envoyer les commandes figurant dans la liste aux périphériques :</p> <pre>https://<serveur de gestion>:<port>/web_api/<commande></pre> <p>show-simple-gateways</p> <p>show-hosts</p> <p>show-networks</p> <p>show-address-ranges</p> <p>show-groups</p> <p>show-groups-with-exclusion</p> <p>show-services-tcp</p> <p>show-services-udp</p> <p>show-service-groups</p> <p>show-packages</p> <p>show-access-rulebase</p> <p>show-nat-rulebase</p> <p>run-script</p> <p>show-task</p>

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 auxquels QRadar Risk Manager peut accéder.

Les fonctions ci-dessous sont disponibles avec l'adaptateur Cisco CatOS :

- Prise en charge des données de voisinage
- Reconnaissance SNMP
- Routage statique
- Protocoles de connexion Telnet et SSH

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

Tableau 13. Exigences d'intégration pour l'adaptateur Cisco CatOS

Exigence d'intégration	Description
Versions	<p>Catalyst série 6500 - périphériques châssis.</p> <p>4.2</p> <p>6.4</p> <p>Restriction : L'adaptateur pour CatOS sauvegarde uniquement la structure de port de commutation essentielle.</p> <p>Les adaptateurs CatOS MSFC (Multilayer Switch Feature Card) sont sauvegardés par des adaptateurs Cisco IOS.</p> <p>Les adaptateurs CatOS (Firewall Services Module) sont sauvegardés par des adaptateurs Cisco ASA.</p>
Reconnaissance SNMP	Correspond à CATOS ou Catalyst Operating System dans SNMP sysDescr.
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Username</p> <p>Password</p> <p>Enable Password</p>
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Utilisez un des protocoles de connexion pris en charge suivants :</p> <p>Telnet</p> <p>SSH</p>

Tableau 13. 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	<p>show version</p> <p>whichboot</p> <p>show module</p> <p>show mod ver</p> <p>show system</p> <p>show flash devices</p> <p>show flash ...</p> <p>show snmp ifalias</p> <p>show port ifindex</p> <p>show interface</p> <p>show port</p> <p>show spantree</p> <p>show ip route</p> <p>show vlan</p> <p>show vtp domain</p> <p>show arp</p> <p>show cdp</p> <p>show cam dynamic</p> <p>show port status</p> <p>show counters</p>

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.

Les fonctions ci-dessous sont disponibles avec l'adaptateur Cisco IOS :

- Prise en charge des données de voisinage
- Conversion d'adresses réseau (NAT) dynamique
- Conversion d'adresses réseau statique (NAT) statique
- Reconnaissance SNMP
- Routage statique
- Routage dynamique EIGRP et OSPF
- Tunnelage P2P/VPN
- Protocoles de connexion Telnet et SSH

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

Tableau 14. Exigences d'intégration pour Cisco IOS

Exigence d'intégration	Description
Versions	<p>IOS 12.0 à 15.1 pour les routeurs et les commutateurs</p> <p>Commutateurs Cisco Catalyst 6500 avec MSFC.</p> <p>Utilisez l'adaptateur Cisco IOS pour sauvegarder la configuration et l'état des services de carte MSFC.</p> <p>Si un routeur Cisco IOS série 7600 dispose d'un FWSM, utilisez l'adaptateur Cisco ASA pour sauvegarder le FWSM.</p>
Niveau d'accès utilisateur	<p>Utilisateur avec un niveau de privilège d'exécution pour les commandes requises par l'adaptateur pour la connexion et la collecte de données. Par exemple, vous pouvez configurer un niveau de privilège 10 personnalisé qui utilise l'authentification de base de données locale.</p> <p>L'exemple suivant attribue aux commandes show ip le niveau de privilège 10.</p> <pre>privilege exec level 10 show ip</pre>
Reconnaissance SNMP	Correspond à ISO ou Cisco Internet Operation System dans SNMP sysDescr.
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Username</p> <p>Password</p> <p>Enable Username (Facultatif)</p> <p>Utilisez cette zone si l'utilisateur a besoin d'indiquer un niveau de privilège spécifique lors de la connexion à l'unité. Utilisez le format <code>level-<n></code> où <i>n</i> est un niveau de privilège [0-15]. Par exemple, pour entrer le niveau de privilège 10, utilisez la commande suivante :</p> <pre>level-10</pre> <p>La commande enable 10 est alors envoyée à l'unité Cisco.</p> <p>Enable Password (Facultatif)</p>
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Utilisez un des protocoles de connexion pris en charge suivants :</p> <p>Telnet</p> <p>SSH</p>

Tableau 14. Exigences d'intégration pour Cisco IOS (suite)

Exigence d'intégration	Description
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	<pre> show access-lists show cdp neighbors detail show diag show diagbus show file systems show glbp show install running show interfaces show inventory show ip route ospf show mac address-table dynamic show module show mod version show object-group show power show snmp show spanning-tree show standby show startup-config show version show vlan show vrrp show vtp status </pre>

Tableau 14. Exigences d'intégration pour Cisco IOS (suite)

Exigence d'intégration	Description
Commandes show ip nécessaires à l'adaptateur pour se connecter et collecter des données	<pre>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 interface show ip ospf neighbor show ip protocols show ip route eigrp terminal length 0</pre>

Cisco Nexus

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

Les fonctions ci-dessous sont disponibles avec l'adaptateur Cisco Nexus :

- Prise en charge des données de voisinage
- Reconnaissance SNMP
- Routage dynamique EIGRP et OSPF
- Routage statique
- Protocoles de connexion Telnet et SSH

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

Tableau 15. Exigences d'intégration pour l'adaptateur Cisco Nexus

Exigence d'intégration	Description
Versions et niveaux de système d'exploitation pris en charge	<p>Nexus 5548 : système d'exploitation niveau 6.0</p> <p>Nexus 7000 series : système d'exploitation niveau 6.2</p> <p>Nexus 9000 series : système d'exploitation niveau 6.1</p>
Reconnaissance SNMP	<p>Correspond à <i>Cisco NX-OS</i> et une chaîne de qualification facultative qui se termine par <i>Software</i> dans SNMP sysDescr.</p> <p>Exemple : (<i>Cisco NX\ -OS.* Software</i>)</p>

Tableau 15. Exigences d'intégration pour l'adaptateur Cisco Nexus (suite)

Exigence d'intégration	Description
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Username</p> <p>Password</p> <p>Enable Password</p> <p>Si vous ajoutez des contextes d'unité virtuelle (VDC) en tant qu'unités individuelles, vérifiez que les données d'identification requises autorise les actions suivantes :</p> <p style="padding-left: 40px;">Accéder au compte activé pour les VDC.</p> <p style="padding-left: 40px;">Utiliser les commandes requises dans ce contexte virtuel.</p>
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Utilisez un des protocoles de connexion pris en charge suivants :</p> <p>Telnet</p> <p>SSH</p>

Tableau 15. Exigences d'intégration pour l'adaptateur Cisco Nexus (suite)

Exigence d'intégration	Description
<p>Commandes nécessaires à l'adaptateur pour se connecter et collecter des données</p>	<p>show hostname</p> <p>show version</p> <p>show vdc</p> <p>show vdc current-vdc</p> <p>switchto vdc <vdc> où <i>vdc</i> est un contexte vdc actif s'affichant lorsque vous entrez la commande show vdc.</p> <p>show snmp</p> <p>dir <system_fichiers> où <i>system_fichiers</i> est bootflash, slot0, volatile, log, logflash ou system.</p> <p>show running-config</p> <p>show startup-config</p> <p>show module</p> <p>show interface brief</p> <p>show interface snmp-ifindex</p> <p>show ip access-lists</p> <p>show vlan</p> <p>show vtp status</p> <p>show spanning-tree summary</p> <p>show object-group</p> <p>show interface <interface> où <i>interface</i> correspond à toute interface s'affichant lorsque vous entrez la commande show running-config.</p> <p>show hsrp</p> <p>show vrrp</p> <p>show vtp</p> <p>show glbp</p> <p>show ip eigrp</p> <p>show ip route eigrp</p> <p>show ip ospf</p> <p>show ip route ospf</p> <p>show ip rip</p> <p>show ip route rip</p>

Tableau 15. Exigences d'intégration pour l'adaptateur Cisco Nexus (suite)

Exigence d'intégration	Description
Commandes de télémétrie	<pre>terminal length 0</pre> <pre>show hostname</pre> <pre>show vdc</pre> <p>switchto vdc <vdc> où <i>vdc</i> est un contexte vdc actif s'affichant lorsque vous entrez la commande show vdc.</p> <pre>show cdp entry all</pre> <pre>show interface brief</pre> <pre>show ip arp</pre> <pre>show mac address-table</pre> <pre>show ip route</pre>

Méthodes d'ajout de VDC pour les unités Cisco Nexus

Utilisez 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 vous ajoutez des VDC en tant qu'unités virtuelles, chaque VDC s'affiche comme unité dans la topologie.

Si vous ajoutez des VDC en tant que sous-unités, elles s'affichent dans la topologie. Vous pouvez les afficher dans la fenêtre du moniteur de configuration.

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

Utilisez Configuration Source Management pour ajouter des VDC en tant que sous-unités de votre unité Cisco Nexus.

Procédure

1. Activez les commandes suivantes pour l'utilisation spécifiée dans les données d'identification :

- show vdc (contexte admin)
- switchto vdc *x*, où *x* correspond au 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*.

2. Utilisez Configuration Source Management pour ajouter l'adresse IP de *contexte d'admin* de l'unité Nexus.

Pour plus d'informations, voir «Ajout d'une unité réseau», à la page 9.

Ajout de VDC en tant qu'unités individuelles

Utilisez Configuration Source Management 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 Configuration Source Management pour ajouter l'adresse IP admin de chaque VDC.
Pour plus d'informations, voir «Ajout d'une unité réseau», à la page 9.
2. Utilisez Configuration Source Management 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 3 permit command terminal
NexusDevice(config-role)# rule 4 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.

Les fonctions ci-dessous sont disponibles avec l'adaptateur Cisco Security Appliances :

- Prise en charge des données de voisinage
- Conversion d'adresses réseau statique (NAT) statique
- Reconnaissance SNMP
- Routage dynamique EIGRP et OSPF
- Routage statique
- Tunnelage IPSEC
- Protocoles de connexion Telnet et SSH

L'adaptateur Cisco Security Appliances collecte des configurations d'unité en sauvegardant des unités de la famille Cisco. L'adaptateur Cisco Security Appliances prend en charge les pare-feux suivants :

- Cisco Adaptive Security Appliances (ASA) série 5500
- Module FWSM (Firewall Service Module)
- Module sur un châssis Catalyst
- Unité PIX (Private Internet Exchange) établie

Remarque : Les contextes transparents Cisco ASA ne peuvent pas être placés dans la topologie QRadar Risk Manager, et vous ne pouvez pas créer de recherche de chemin sur ces contextes transparents.

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

Tableau 16. Exigences d'intégration pour l'adaptateur Cisco Security Appliances

Exigence d'intégration	Description
Versions	ASA : 8.2, 8.4 à 9.1.7 PIX : 6.1, 6.3 FWSM : 3.1, 3.2
Niveau d'accès utilisateur minimum	Niveau de privilège 5 Vous pouvez sauvegarder des unités avec un niveau d'accès de niveau de privilège 5. Par exemple, vous pouvez configurer un utilisateur de niveau 5 qui utilise l'authentification de base de données locale en exécutant les commandes suivantes : aaa authorization command LOCAL aaa authentication enable console LOCAL privilege cmd level 5 mode exec command terminal privilege cmd level 5 mode exec command changeto (multi-context only) privilege show level 5 mode exec command running-config privilege show level 5 mode exec command startup-config privilege show level 5 mode exec command version privilege show level 5 mode exec command shun privilege show level 5 mode exec command names privilege show level 5 mode exec command interface privilege show level 5 mode exec command pager privilege show level 5 mode exec command arp privilege show level 5 mode exec command route privilege show level 5 mode exec command context privilege show level 5 mode exec command mac-address-table
Reconnaissance SNMP	Correspond à PIX ou Adaptive Security Appliance ou Firewall Service Module dans SNMP sysDescr.

Tableau 16. Exigences d'intégration pour l'adaptateur Cisco Security Appliances (suite)

Exigence d'intégration	Description
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Username</p> <p>Password</p> <p>Enable Password</p> <p>Vous pouvez définir le niveau d'activation de l'utilisateur que vous configurez pour accéder à l'unité ASA à partir de QRadar Risk Manager. Par exemple, utilisez le nom d'utilisateur d'activation de level-5 pour faire en sorte que l'adaptateur exécute enable 5 afin de passer en mode privilégié et non en mode d'activation supérieur.</p>
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Utilisez un des protocoles de connexion pris en charge suivants :</p> <p>Telnet</p> <p>SSH</p> <p>SCP</p>

Tableau 16. Exigences d'intégration pour l'adaptateur Cisco Security Appliances (suite)

Exigence d'intégration	Description
Commandes requises par l'adaptateur pour la connexion et la collecte de données	<pre> changeto context <context> changeto system show running-config show startup-config show arp show context show interface show mac-address-table show names show ospf neighbor show route show shun show version terminal pager 0 show interface detail show crypto ipsec sa show eigrp topology show eigrp neighbors show firewall </pre> <p>La commande <code>changeto context <context></code> est utilisée pour chaque contexte de l'unité ASA.</p> <p>La commande <code>changeto system</code> détecte si le système possède des configuration <i>multi-contexte</i> et détermine le <i>contexte-admin</i>.</p> <p>La commande <code>changeto context</code> est requise si la commande <code>changeto system</code> possède une configuration <i>multi-contexte</i> ou un contexte <i>configuration-admin</i>.</p> <p>La commande <code>terminal pager</code> est utilisée pour désactiver le comportement de pagination.</p>

F5 BIG-IP

IBM Security QRadar Risk Manager prend en charge l'adaptateur F5 BIG-IP.

Les fonctions ci-dessous sont disponibles avec l'adaptateur F5 BIG-IP :

- Prise en charge des données de voisinage
- Conversion d'adresses réseau (NAT) dynamique

- Conversion d'adresses réseau statique (NAT) statique
- Reconnaissance SNMP
- Routage statique
- Protocoles de connexion Telnet et SSH

Les dispositifs d'équilibrage de charge F5 BIG-IP qui exécutent LTM (Local Traffic Manager) sont pris en charge.

Sur le dispositif F5 BIG-IP, vous devez configurer le rôle **Admin** pour le nom d'utilisateur utilisé par QRadar Risk Manager pour la sauvegarde et configure **Advanced Shell** pour **Terminal Access**.

Le tableau ci-dessous décrit les exigences d'intégration pour l'adaptateur F5 BIG-IP.

Tableau 17. Exigences d'intégration pour l'adaptateur F5 BIG-IP

Exigence d'intégration	Description
Versions	10.1.1 11.4.1
Reconnaissance SNMP	Correspond à F5 BIG-IP dans SNMP sysDescr
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	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 17. Exigences d'intégration pour l'adaptateur F5 BIG-IP (suite)

Exigence d'intégration	Description
<p>Commandes nécessaires à l'adaptateur pour se connecter et collecter des données bigpipe</p>	<p>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</p>
<p>Commandes nécessaires à l'adaptateur pour se connecter et collecter des données</p>	<p>b db snat.anyipprotocol</p>

Tableau 17. Exigences d'intégration pour l'adaptateur F5 BIG-IP (suite)

Exigence d'intégration	Description
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données tmsh	<pre> 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 </pre>
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données tmsh (suite)	<pre> 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 </pre>
Fichiers collectés	<pre> /config/bigip.license /config/snmp/snmpd.conf /etc/passwd </pre>

Fortinet FortiOS

L'adaptateur IBM Security QRadar Risk Manager pour Fortinet FortiOS prend en charge les dispositifs Fortinet FortiGate permettant l'exécution du système d'exploitation Fortinet (FortiOS).

Les fonctions ci-dessous sont disponibles avec l'adaptateur Fortinet FortiOS :

- Conversion d'adresses réseau statique (NAT) statique
- Routage statique
- Protocoles de connexion Telnet et SSH

L'interaction entre l'adaptateur Fortinet FortiOS et FortiOS se fait par Telnet ou SSH. La liste ci-dessous décrit certaines limitations de QRadar Risk Manager et de l'adaptateur Fortinet FortiOS :

- Les adresses géographiques et les règles référencées ne sont pas prises en charge par QRadar Risk Manager.
- Les règles de sécurité basées sur l'identité, le VPN et le protocole IP ne sont pas prises en charge par QRadar Risk Manager.
- Les règles utilisant des profils Unified Threat Management (UTM) ne sont pas prises en charge par l'adaptateur Fortinet FortiOS. Seules les règles de pare-feu de la couche 3 sont prises en charge.
- Les routes de règle ne sont pas prises en charge.
- Les domaines virtuels avec des liens virtuels avec des adresses IP partielles ou sans adresses IP ne sont pas pris en charge.

Les exigences d'intégration de l'adaptateur Fortinet FortiOS sont décrites dans le tableau ci-dessous :

Tableau 18. Exigences d'intégration pour l'adaptateur Fortinet FortiOS

Exigence d'intégration	Description
Version	Versions 4.0 MR3 à 5.2.4
Reconnaissance SNMP	Non
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Utilisez un des protocoles de connexion pris en charge suivants : Telnet SSH
Exigences de niveau d'accès utilisateur	Accès en lecture-écriture pour les pare-feu Fortinet avec des VDOM actifs Accès en lecture seule pour les pare-feu Fortinet sans VDOM actifs

Tableau 18. Exigences d'intégration pour l'adaptateur Fortinet FortiOS (suite)

Exigence d'intégration	Description
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	<p>config system console</p> <p>set output standard</p> <p>Remarque : Les commandes config system console et set output standard doivent être utilisées par un utilisateur possédant des droits d'accès en lecture et en écriture sur la configuration du système. Si cet utilisateur est en lecture seule avec mise en page activée au moment de la sauvegarde d'un périphérique Fortigate, les performances seront considérablement affectées.</p> <p>show system interface</p> <p>get hardware nic <variable></p> <p>get system status</p> <p>get system performance status</p> <p>get router info routing-table static</p> <p>get test dnsproxy 6</p> <p>show firewall addrgrp</p> <p>show firewall address</p> <p>show full-configuration</p> <p>get firewall service predefined <variable></p> <p>show firewall service custom</p> <p>show firewall service group</p> <p>show firewall policy</p> <p>show system zone</p> <p>show firewall vip</p> <p>show firewall vipgrp</p> <p>show firewall ippool</p>
Commandes à utiliser avec les VDOM	<p>config global pour entrer dans le mode de configuration globale</p> <p>config vdom; edit <nom-vdom> pour passer d'un VDOM à l'autre.</p>

Adaptateur SNMP générique

IBM Security QRadar Risk Manager prend en charge les dispositifs qui exécutent un agent SNMP avec l'adaptateur SNMP générique.

Cet adaptateur interagit avec l'agent SNMP à l'aide de requêtes SNMP.

Les identificateurs d'objet (OID) figurent dans SNMP MIB-2, et vous pouvez attendre de tous les agents SNMP qu'ils exposent ces OID.

L'adaptateur présente les limitations suivantes :

- Il collecte uniquement les informations de l'interface de base et du système de base. Les informations de règle et de routage ne sont pas collectées.
- Même s'il est affiché dans l'interface utilisateur **Configuration Source Management**, avec SNMPv3, l'adaptateur ne prend pas en charge le chiffrement AES.
- L'adaptateur ne prend pas en charge le chiffrement AES avec SNMPv3, même s'il semble qu'il soit pris en charge dans la fenêtre Configuration Source Management.

Les exigences d'intégration pour l'adaptateur SNMP générique sont décrites dans le tableau suivant :

Exigence d'intégration	Description
Version	SNMPv1, SNMPv2c, SNMPv3
Prise en charge des données de voisinage	Non
Reconnaissance SNMP	Non
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	SNMPv1 et SNMPv2c requièrent SNMP Get Community SNMPv3 requiert SNMPv3 Authentication Username SNMPv3 peut avoir l'une des données d'identification suivantes : SNMPv3 Authentication Password SNMPv3 Privacy Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Utilisez un des protocoles de connexion pris en charge suivants : SNMPv1 SNMPv2c SNMPv3 avec MD5 SHA avec DES

Exigence d'intégration	Description
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	Commandes Get SNMP
	.1.3.6.1.2.1.1.1.0
	.1.3.6.1.2.1.1.2.0
	.1.3.6.1.2.1.1.3.0
	.1.3.6.1.2.1.1.4.0
	.1.3.6.1.2.1.1.5.0
	.1.3.6.1.2.1.1.6.0
	Commandes Walk SNMP
	.1.3.6.1.2.1.2.2.1.2
	.1.3.6.1.2.1.2.2.1.3
	.1.3.6.1.2.1.2.2.1.4
	.1.3.6.1.2.1.2.2.1.5
	.1.3.6.1.2.1.2.2.1.6
	.1.3.6.1.2.1.2.2.1.7
.1.3.6.1.2.1.4.20	

HP Networking ProVision

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

Les fonctions ci-dessous sont disponibles avec l'adaptateur HP Networking ProVision :

- Prise en charge des données de voisinage
- Reconnaissance SNMP
- Routage dynamique RIP
- Protocoles de connexion Telnet et SSH

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

Tableau 19. Exigences d'intégration pour l'adaptateur HP Networking ProVision

Exigence d'intégration	Description
Versions	HP Networking ProVision Switches K/KA.15.X Restriction : Les commutateurs HP sous système d'exploitation Comware ne prennent pas en charge cet adaptateur.
Reconnaissance SNMP	Correspond aux numéros de version au format HP(.*)Switch(.*) (révision [A-Z]{1,2}\.(\d+)\.(\d+)) dans sysDescr.

Tableau 19. Exigences d'intégration pour l'adaptateur HP Networking ProVision (suite)

Exigence d'intégration	Description
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Username</p> <p>Password</p> <p>Enable Password</p>
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>SSH</p>

Tableau 19. Exigences d'intégration pour l'adaptateur HP Networking ProVision (suite)

Exigence d'intégration	Description
<p>Commandes d'opération de sauvegarde émises par l'adaptateur à destination de l'unité</p>	<pre> dmesgshow system power-supply getmib show access-list vlan <id vlan> show access-list show access-list <nom ou numéro> show access-list ports <numéro de port> show config show filter show filter <id> show running-config show interfaces brief show interfaces <id interface> pour chaque interface. show jumbos show trunks show lacp show module show snmp-server show spanning-tree show spanning-tree config show spanning-tree instance <id ou liste> (pour chaque spanning-tree qui est 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 </pre>

Tableau 19. 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	<pre>show ip show ip route show ip odpf show ip odpf redistribute show ip rip show ip rip redistribute</pre>
Commandes de télémétrie et de données de voisinage	<pre>getmib show arp show cdp neighbors show cdp neighbors detail <numéro de port> show interfaces brief show interface show ip route show lldp info remote-device show lldp info remote-device <numéro de port> show mac-address or show mac address show system information show vlans show vlans custom id state ipaddr ipmask walkmib</pre>

Juniper Networks JUNOS

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

Les fonctions ci-dessous sont disponibles avec l'adaptateur Juniper Networks JUNOS :

- Prise en charge des données de voisinage
- Reconnaissance SNMP
- Routage dynamique OSPF
- Routage statique
- Protocoles de connexion Telnet et SSH

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

Tableau 20. Exigences d'intégration pour l'adaptateur Juniper Networks JUNOS

Exigence d'intégration	Description
Versions	10.4 11.2 vers 12.3 13.2
Reconnaissance SNMP	Correspond à SNMP sysOID: 1.3.6.1.4.1.2636
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Utilisez un des protocoles de connexion pris en charge suivants : Telnet SSH SCP

Tableau 20. Exigences d'intégration pour l'adaptateur Juniper Networks JUNOS (suite)

Exigence d'intégration	Description
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	<pre> 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 route protocol bgp show ospf interface detail show bgp neighbor show configuration routing-option show arp no-resolve show ospf neighbor show rip neighbor </pre>

Juniper Networks NSM

L'adaptateur IBM Security QRadar Risk Manager prend en charge Juniper Networks NSM (Network and Security Manager).

Vous pouvez utiliser QRadar Risk Manager pour sauvegarder une unité Juniper Networks unique ou pour obtenir des informations sur une 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.

Vous pouvez utiliser les protocoles de connexion HTTPS et SOAP avec Juniper Networks NSM.

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

Tableau 21. 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
Reconnaissance SNMP	Pas de prise en charge
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Utilisez un des protocoles de connexion pris en charge suivants : 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.

Les fonctions ci-dessous sont disponibles avec l'adaptateur Juniper Networks ScreenOS :

- Prise en charge des données de voisinage
- Conversion d'adresses réseau (NAT) dynamique
- Conversion d'adresses réseau statique (NAT) statique
- Reconnaissance SNMP
- Routage statique
- Protocoles de connexion Telnet et SSH

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

Tableau 22. Exigences d'intégration pour l'adaptateur Juniper Networks ScreenOS

Exigence d'intégration	Description
Versions	5.4 6.2
Reconnaissance SNMP	Correspond à netscreen ou SSG dans SNMP sysDescr.
Paramètres de données d'identification obligatoires	Username Password

Tableau 22. Exigences d'intégration pour l'adaptateur Juniper Networks ScreenOS (suite)

Exigence d'intégration	Description
Protocoles de connexion pris en charge	Utilisez un des protocoles de connexion pris en charge suivants : Telnet SSH
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 addresszone <i>groupe</i> get address
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données (suite)	get service group get service group <i>variable</i> get interface get interface <i>variable</i> get policy all get policy id <i>variable</i> get admin user get route get arp get mac-learn get counter statistics interface <i>variable</i> Où <i>zone</i> correspond aux données de zone renvoyées par la commande get config. <i>groupe</i> correspond aux données de groupe renvoyées par la commande get config. <i>variable</i> 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 l'interface de programme d'application (API) Rest XML PAN-OS pour communiquer avec les périphériques pare-feu Palo Alto.

Les fonctions ci-dessous sont disponibles avec l'adaptateur Palo Alto :

- Prise en charge des données de voisinage
- Conversion d'adresses réseau (NAT) dynamique
- Conversion d'adresses réseau statique (NAT) statique
- Routage statique
- Reconnaissance SNMP
- Tunnelage IPSEC/VPN
- Applications
- Utilisateur/Groupes
- Protocole de connexion HTTPS

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

Tableau 23. Exigences d'intégration pour l'adaptateur Palo Alto

Exigence d'intégration	Description
Versions	Versions PAN-OS 5.0 à 7.0
Niveau d'accès utilisateur minimum	Accès superutilisateur (accès complet) requis pour les unités PA qui comportent des listes de blocs dynamiques pour exécuter des commandes de niveau système. Accès superutilisateur (en lecture seule) pour toutes les autres unités PA.
Reconnaissance SNMP	SysDescr correspond à 'Palo Alto Networks(*)series firewall' ou sysOid correspond à 'panPA'
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	HTTPS

Tableau 23. Exigences d'intégration pour l'adaptateur Palo Alto (suite)

Exigence d'intégration	Description
Commandes devant être utilisées pour l'opération de sauvegarde.	<pre>/api/?type=op&cmd=<show><system><info></info></system>/show></pre> <pre>/api/?type=op&cmd=<show><config><running></running></config></show></pre> <pre>/api/?type=op&cmd=<show><interface>all</interface></show></pre>
Commandes facultatives à utiliser pour l'opération de sauvegarde	<pre>/api/?type=op&cmd=<show><system><resources></resources></system></show></pre> <pre>/api/?type=op&cmd=/config/predefined/service</pre> <pre>/api/?type=op&cmd=<request><system><external-list><show><name>\${listName}</name>< /show></external-list></system></request> où <i>listName</i> est une variable dans cette commande, qui s'exécute plusieurs fois.</pre> <pre>/api/?type=op&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show></pre> <pre>/api/?type=config&action=get&xpath=/config/predefined/application</pre>
Commandes devant être utilisées pour la télémétrie et les données de voisinage.	<pre>/api/?type=op&cmd=<show><system><info></info></system></show></pre> <pre>/api/?type=op&cmd=<show><interface>all</interface></show></pre> <pre>/api/?type=op&cmd=<show><routing><interface></interface></routing></show></pre>
Commandes facultatives à utiliser pour la télémétrie et les données de voisinage.	<pre>/api/?type=op&cmd=<show><counter><interface>all</interface></counter></show></pre> <pre>/api/?type=op&cmd=<show><arp>all</arp></show></p><p><show><mac>all</mac></show></pre> <pre>/api/?type=op&cmd=<show><arp>all</arp></show></pre> <pre>/api/?type=op&cmd=<show><routing><route></route></routing></show></pre>
Commandes devant être utilisées pour GetApplication.	<pre>/api/?type=config&action=get&xpath=/config/predefined/application</pre>

Tâches associées:

«Ajout d'unités gérées par Palo Alto Panorama», à la page 15
 Utilisez Configuration Source Management pour ajouter à IBM Security QRadar Risk Manager des unités provenant de Palo Alto Panorama.

Sidewinder

IBM Security QRadar Risk Manager prend en charge les dispositifs McAfee Enterprise Firewall (Sidewinder) qui exécutent SecureOS.

Les fonctions ci-dessous sont disponibles avec l'adaptateur Sidewinder :

- Conversion d'adresses réseau statique (NAT) statique
- Routage statique
- Protocoles de connexion Telnet et SSH

L'adaptateur Sidewinder interagit avec le système d'exploitation McAfee basé sur une interface CLI (SecureOS) sur Telnet ou SSH.

L'adaptateur Sidewinder possède les limitations suivantes :

- Seules les règles d'administration de pare-feu Layer 3 sont prises en charge car les règles Layer 7 qui utilisent les défenses d'application Sidewinder ne sont pas prises en charge.
- Les règles basées sur l'identité, la zone géographique et les règles IPv6 sont abandonnées car elle ne sont pas prises en charge par QRadar Risk Manager.

Les exigences d'intégration pour l'adaptateur Sidewinder sont décrites dans le tableau suivant :

Tableau 24. Adaptateur Sidewinder

Exigence d'intégration	Description
Versions prises en charge	8.3.2
Niveau d'accès utilisateur minimum	admin Le niveau d'accès administrateur est requis pour l'extraction des informations de services prédéfinies de la base de données à l'aide de la commande cf appdb list verbose=on .
Reconnaissance SNMP	Non
Paramètres de données d'identification obligatoires	Username Password
Protocoles de connexion pris en charge	Utilisez un des protocoles de connexion pris en charge suivants : SSH Telnet

Tableau 24. Adaptateur Sidewinder (suite)

Exigence d'intégration	Description
Commandes nécessaires à l'adaptateur pour se connecter et collecter des données	<pre>hostname uname -r uptime cf license q cf route status cf ipaddr q cf iprange q cf subnet q cf domain q Use "dig \$address +noall +answer" for each domain output from: cf domain q cf host q cf netmap q cf netgroup q cf appdb list verbose=on cf application q cf appgroup q cf policy q cf interface q cf zone q</pre>

Sourcefire 3D Sensor

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

Les fonctions ci-dessous sont disponibles avec l'adaptateur Sourcefire 3D Sensor :

- IPS
- Protocole de connexion SSH

Limitations :

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

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

Tableau 25. Exigences d'intégration pour l'adaptateur Sourcefire 3D Sensor

Exigence d'intégration	Description
Versions	5.2
Modèles 3D Sensors pris en charge (unités Series 2)	3D500 3D1000 3D2000 3D2100 3D2500 3D3500 3D4500 3D6500 3D9900
Reconnaissance SNMP	Non
Paramètres de données d'identification obligatoires Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	Username Password
Protocoles de connexion pris en charge Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin .	SSH

Tableau 25. Exigences d'intégration pour l'adaptateur Sourcefire 3D Sensor (suite)

Exigence d'intégration	Description
<p>Commandes nécessaires à l'adaptateur pour se connecter et collecter des données</p>	<p>show version</p> <p>show memory</p> <p>show network</p> <p>show interfaces</p> <p>expert</p> <p>sudo</p> <p>su</p> <p>df</p> <p>hostname</p> <p>ip addr</p> <p>route</p> <p>cat</p> <p>find</p> <p>head</p> <p>mysql</p>
<p>Commandes utilisées par l'adaptateur pour lire les informations de configuration :</p> <p>Obtention d'informations matérielles.</p> <p>Obtention du nom d'hôte du système.</p> <p>Obtention d'informations de routage.</p> <p>Utilisation de la commande cat ou head pour lire des fichiers et obtenir des configurations.</p> <p>Obtention du répertoire de base de l'instance SNORT, référencée sous la forme \$DE_DIR dans les trois exemples suivants :</p> <p>Lecture des objets et des règles IPS.</p> <p>Lecture de la configuration SNORT.</p> <p>Les fichiers sont lus dynamiquement lorsqu'ils sont référencés dans le fichier policyText_full.yaml.</p> <p>L'adaptateur utilise la commande find pour rechercher des fichiers de réputation IP dans ce répertoire.</p>	<p>sudo su df</p> <p>sudo su hostname</p> <p>sudo su route -n</p> <p>/etc/sf/ims.conf</p> <p>\$SNORT_DIR/fwcfg/affinity.conf</p> <p>\$DE_DIR/policyText_full.yaml</p> <p>\$DE_DIR/snort.conf</p> <p>\$DE_DIR/*</p> <p>\$SNORT_DIR/iprep_download</p>

Tableau 25. Exigences d'intégration pour l'adaptateur Sourcefire 3D Sensor (suite)

Exigence d'intégration	Description
Fichier comportant les données d'identification pour la connexion à la base de données.	/etc/sf/ims-data.conf

Adaptateur IPS TippingPoint

IBM Security QRadar Risk Manager prend en charge les dispositifs IPS (système de prévention contre les intrusions) TippingPoint qui exécutent TOS et sont sous contrôle SMS.

Les fonctions ci-dessous sont disponibles avec l'adaptateur TippingPoint IPS :

- IPS
- Protocoles de connexion Telnet et SSH+HTTPS

Cet adaptateur requiert une interaction avec les périphériques suivants :

- Directement avec le système de prévention contre les intrusions (IPS) par l'utilisation du système d'exploitation TippingPoint (TOS) sur Telnet ou SSH.
- TippingPoint Secure Management Server (SMS) via les services Web API sur HTTPS.

Une connexion au serveur SMS TippingPoint est nécessaire pour obtenir les signatures Digital Vaccines les plus récentes, lesquelles sont gérées par le serveur SMS.

Cet adaptateur est compatible uniquement avec les périphériques IPS sous contrôle SMS. Les services Web SMS doivent être activés pour une sauvegarde réussie.

Cette liste répertorie les limitations de l'adaptateur TippingPoint :

- QRadar Risk Manager ne traite pas les adresses IP source et cible dans les règles ou les filtres IPS. Les fonctions TippingPoint suivantes ne sont pas prises en charge :
 - Filtres de gestion du trafic
 - Exceptions et restrictions de profil ou de filtre
 - Filtres définis par l'utilisateur
- Les filtres IPS sans CVE associé ne sont pas modélisés car le système de prévention contre les intrusions ne peut être mappé à aucune vulnérabilité QRadar.

Les exigences d'intégration pour l'adaptateur TippingPoint sont décrites dans le tableau suivant :

Tableau 26. Adaptateur IPS TippingPoint

Exigence d'intégration	Description
Versions prises en charge	TOS 3.6 et SMS 4.2
Niveau d'accès utilisateur minimum	IPS : opérateur SMS : opérateur (personnalisé) Utilisateur qui appartient à un groupe avec un rôle <i>opérateur personnalisé</i> , et dont l'option Accès aux services Web SMS est activée.

Tableau 26. Adaptateur IPS TippingPoint (suite)

Exigence d'intégration	Description
Reconnaissance SNMP	Non
<p>Paramètres de données d'identification obligatoires</p> <p>Pour ajouter des données d'identification dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Entrez les données d'identification suivantes :</p> <p>Nom d'utilisateur: <nom utilisateur IPS CLI></p> <p>Mot de passe: <mot de passe IPS CLI></p> <p>Nom d'utilisateur d'activation: <nom utilisateur SMS></p> <p>Mot de passe d'activation: <mot de passe SMS></p>
<p>Protocoles de connexion pris en charge</p> <p>Pour ajouter des protocoles dans QRadar, connectez-vous en tant qu'administrateur et utilisez Configuration Source Management sous l'onglet Admin.</p>	<p>Utilisez un des protocoles de connexion pris en charge suivants :</p> <p>Telnet pour IPS CLI</p> <p>SSH pour IPS CLI</p> <p>HTTPS pour SMS</p>
<p>Commandes nécessaires à l'adaptateur pour se connecter et collecter des données</p>	<p>show config</p> <p>show version</p> <p>show interface</p> <p>show host</p> <p>show sms</p> <p>show filter \$filterNumber (pour chaque signature trouvée dans Digital Vaccine)</p>
<p>Commandes API envoyées à SMS pour extraire les signatures les plus récentes</p>	<p>https://<serveur_sms>/dbAccess/tptDBServlet?method=DataDictionary&table=SIGNATURE&format=xml</p>

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEF AUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

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

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 de données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

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

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

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

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

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

Dispositions relatives à la documentation du produit

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

Applicabilité

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

Utilisation personnelle

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

Utilisation commerciale

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE

Déclaration IBM de confidentialité en ligne

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

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

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (<http://www.ibm.com/privacy/fr/fr>) et la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site <http://www.ibm.com/privacy/details/fr/fr>, ainsi que la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site <http://www.ibm.com/software/info/product-privacy> (en anglais).

