IBM Security QRadar Risk Manager
Version 7.2.4

Guide d'installation

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations fournies à la section «Remarques», à la page 27.

Ce document s'applique à IBM QRadar Security Intelligence Platform V7.2.4 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Présentation de l'installation d'IBM Security QRadar Risk Manager

Ces informations sont destinées à une utilisation avec IBM® Security QRadar Risk Manager. QRadar Risk Manager est un dispositif utilisé pour contrôler les configurations d'unité, simuler les changements apportés à votre environnement réseau et classer les risques et vulnérabilités par ordre de priorité sur votre réseau.

Ce guide contient des instructions pour l'installation de QRadar Risk Manager et l'ajout de QRadar Risk Manager en tant qu'hôte géré sur la console IBM Security QRadar SIEM.

Les logiciels et le système d'exploitation Red Hat Enterprise Linux sont préinstallés sur les dispositifs QRadar Risk Manager. Vous pouvez également installer le logiciel QRadar Risk Manager sur votre propre matériel.

Utilisateurs concernés

Ce guide est destiné aux administrateurs de réseau responsables de l'installation et de la configuration des systèmes QRadar Risk Manager sur votre réseau.

Les administrateurs doivent avoir une connaissance pratique de la mise en réseau et des systèmes Linux.

Documentation technique

Pour savoir comment accéder à plus de documentation technique, aux notes techniques et aux notes sur l'édition, voir Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21612861).

Contacter le service clients

Pour contacter le service clients, voir Support and Download Technical Note (en anglais) (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. Un accès non autorisé peut se traduire par la modification, la destruction ou le détournement d'informations, ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE

VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Chapitre 1. Préparation à l'installation d'IBM Security QRadar Risk Manager

Vous pouvez installer un dispositif IBM Security QRadar Risk Manager en tant qu'hôte géré sur votre console IBM Security QRadar. Un seul exemple de QRadar Risk Manager peut exister sur une console QRadar.

A compter de la version 7.1 de QRadar Risk Manager, la console QRadar et QRadar Risk Manager utilisent les mêmes processus d'installation et ISO pour l'installation. C'est pourquoi vous pouvez utiliser l'éditeur de déploiement de la console QRadar pour ajouter QRadar Risk Manager à votre déploiement. Une installation de dispositif QRadar Risk Manager inclut le logiciel QRadar Risk Manager et un système d'exploitation Red Hat Enterprise Linux.

Avant de procéder à l'installation

Vous devez exécuter le processus d'installation d'une console IBM Security QRadar avant d'installer IBM Security QRadar Risk Manager. Il est recommandé d'installer QRadar SIEM et QRadar Risk Manager sur le même commutateur réseau.

Pour plus d'informations sur l'installation de QRadar SIEM, y compris les configurations logicielle et matérielle, voir le *guide d'installation d'IBM Security QRadar SIEM*.

IBM Security QRadar Risk Manager étant un dispositif 64 bits, veillez à télécharger le logiciel d'installation approprié à votre système d'exploitation.

Identification des paramètres réseau

Vous devez collecter des informations sur vos paramètres réseau avant de débuter le processus d'installation.

Réunissez les informations suivantes concernant vos paramètres réseau :

- Nom d'hôte
- Adresse IP
- Adresse du masque de réseau
- Masque de sous-réseau
- Adresse de la passerelle par défaut
- Adresse du serveur DNS principal
- Adresse du serveur DNS secondaire (facultatif)
- Adresse IP publique pour les réseaux utilisant un nom de serveur de messagerie NAT
- Nom du serveur de messagerie
- Serveur NTP (Console uniquement) ou nom du serveur d'horloge

Configuration d'accès aux ports sur les pare-feu

Les pare-feux entre la console IBM Security QRadar et IBM Security QRadar Risk Manager doivent autoriser le trafic sur certains ports.

Vérifiez que tout pare-feu situé entre la console QRadar SIEM et QRadar Risk Manager autorise le trafic sur les ports suivants :

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (horloge)

Fonctions non prises en charge dans QRadar Risk Manager

il est important de connaître les fonctions qui ne sont pas prises en charge par IBM Security QRadar Risk Manager.

Les fonctions suivantes ne sont pas prises en charge dans QRadar Risk Manager :

- Haute disponibilité (HA)
- Routage dynamique pour les protocoles BGP (Border Gateway Protocol), OSPF (Open Shortest Path First) ou RIP (protocole de routage).
- IPv6
- Masques de réseau non contigus
- Routes à équilibrage de charge
- Mappes de référence
- Stockage et retransmission

Configuration matérielle supplémentaire

Du matériel supplémentaire est nécessaire avant d'installer IBM Security QRadar Risk Manager.

Avant d'installer des systèmes IBM QRadar Risk Manager, vous devez accéder aux composants matériels suivants :

- moniteur et clavier ou console série
- alimentation de secours (UPS)

Les dispositifs ou systèmes des logiciels QRadar Risk Manager qui exécutent QRadar Risk Manager qui stockent des données doivent être dotés d'une alimentation de secours (UPS). L'utilisation de cette alimentation de secours garantit que vos données QRadar Risk Manager, notamment des consoles, processeurs d'événement et collecteurs QFlow Collector, sont conservées en cas de coupure de courant.

Configuration logicielle supplémentaire

Des logiciels supplémentaires sont nécessaires avant d'installer IBM Security QRadar Risk Manager.

Les logiciels suivants doivent êtres installés sur le système du bureau que vous utilisez pour accéder à l'interface utilisateur de QRadar Risk Manager :

- Environnement d'exécution Java™
- Adobe Flash, version 10 ou supérieure

Navigateurs Web pris en charge

Pour assurer une bonne exécution des fonctions des produits IBM Security QRadar, vous devez utiliser un navigateur Web pris en charge.

Lorsque vous accédez au système QRadar, vous êtes invité à fournir vos nom d'utilisateur et mot de passe. Le nom d'utilisateur et le mot de passe doivent être configurés à l'avance par l'administrateur.

Le tableau suivant répertorie les versions prises en charge des navigateurs Web.

Tableau 1. Navigateurs Web pris en charge par les produits QRadar

Navigateur Web	Versions prises en charge
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer 32 bits, avec mode document et mode navigateur activés	9.0 10.0
Google Chrome	Version en cours à la date d'édition des produits IBM Security QRadar V7.2.4

Activation des modes Document et Navigateur dans Internet Explorer

Si vous utilisez Microsoft Internet Explorer pour accéder aux produits IBM Security QRadar, vous devez activer les modes Document et Navigateur.

Procédure

1. Dans votre navigateur web Internet Explorer, appuyez sur la touche F12 pour ouvrir la fenêtre Outils de développement.
2. Cliquez sur **Mode Navigateur** et sélectionnez la version de votre navigateur web.
3. Cliquez sur **Mode Document**.
   - Pour Internet Explorer 9.0, sélectionnez **Normes d'Internet Explorer 9**.
   - Pour Internet Explorer 10.0, sélectionnez **Normes d'Internet Explorer 10**.

Chapitre 2. Installation de dispositifs IBM Security QRadar Risk Manager

Un déploiement d'IBM Security QRadar Risk Manager inclut une console IBM Security QRadar et le dispositif QRadar Risk Manager en tant qu'hôte géré.

L'installation de QRadar Risk Manager implique les étapes suivantes :

1. Préparation de votre dispositif.
2. Installation de QRadar Risk Manager.
3. Ajout de QRadar Risk Manager à QRadar.

Préparation de votre dispositif

Vous devez préparer votre unité avant d'installer un dispositif IBM Security QRadar Risk Manager.

Avant de commencer

Vous devez installer tout le matériel requis et vous avez besoin d'un clé d'activation. Cette clé d'activation est une chaîne alphanumérique de 24 chiffres répartis en quatre groupes de chiffres, qui vous est fournie par IBM. Où trouver la clé d'activation :

- Imprimée sur un autocollant apposé sur votre dispositif.
- Fournie avec le bordereau de marchandises ; tous les dispositifs y figurent avec leurs clés associées.

Afin d'éviter toute erreur de frappe, la lettre I et le nombre 1 (un) sont traités de manière identique, tout comme la lettre O et le nombre 0 (zéro).

Si vous ne disposez pas d'une clé d'activation pour votre dispositif QRadar Risk Manager, prenez contact avec le service clients (http://www.ibm.com/support).

Pour plus d'informations sur votre dispositif, voir le *guide d'installation du matériel IBM Security QRadar*.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Connectez un ordinateur portable au port série situé à l'arrière du dispositif.

     Si vous utilisez un ordinateur portable pour vous connecter au système, vous devez utiliser un programme de terminal, par exemple HyperTerminal, pour vous connecter au système. Veillez à définir le **mode de connexion** sur le port COM approprié du connecteur en série et les **bits par seconde** sur 9600. Vous devez également définir les **bits d'arrêt** (1), **bits d'information**s (8) et la **parité** (None).
   - Connectez un clavier et un moniteur à leurs ports respectifs.
2. Mettez le système sous tension et connectez-vous. Le nom d'utilisateur, sensible à la casse, est root.
3. Appuyez sur Entrée.

4. Lisez les informations à l'écran. Appuyez sur la barre d'espacement pour passer à l'écran suivant, jusqu'à ce que vous parveniez à la fin du document.
5. Tapez yes pour accepter le contrat, puis appuyez sur Entrée.
6. Entrez votre clé d'activation et appuyez sur Entrée.

Accès à l'interface utilisateur d'IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager utilise les informations de connexion par défaut de l'URL, du nom d'utilisateur et du mot de passe.

Vous accédez à IBM Security QRadar Risk Manager via la console QRadar. Utilisez les informations du tableau suivant lorsque vous vous connectez à votre console IBM Security QRadar.

Tableau 2. Informations de connexion par défaut pour QRadar Risk Manager

Informations de connexion	**Valeur par défaut**
URL	https://<IP address>, où <IP address> est l'adresse IP de la console QRadar.
Nom d'utilisateur	admin
Mot de passe	Mot de passe attribué à QRadar Risk Manager lors du processus d'installation.
Clé de licence	Une clé de licence par défaut fournit l'accès au système pour 5 semaines.

Informations de paramètre réseau pour IPv4

Des informations sur le réseau pour les paramètres de réseau Internet Protocol version 4 (IPv4) sont nécessaires lorsque vous installez IBM Security QRadar Risk Manager ou lorsque vous modifiez les paramètres réseau.

Des informations sur le réseau sont nécessaires lorsque vous installez ou réinstallez IBM Security QRadar Risk Manager, ou lorsque vous devez modifier des paramètres réseau.

Le paramètre de réseau IP public est facultatif. Cette adresse IP secondaire est utilisée pour accéder au serveur, généralement depuis un autre réseau ou depuis Internet, et elle est gérée par votre administrateur de réseau. L'adresse IP publique est souvent configurée via les services NAT (conversion d'adresses réseau) sur votre réseau ou les paramètres de pare-feu sur votre réseau. La conversion d'adresses réseau convertit une adresse IP sur un réseau en une autre adresse IP sur un autre réseau.

Installation d'IBM Security QRadar Risk Manager

Vous pouvez installer IBM Security QRadar Risk Manager une fois que vous avez préparé votre dispositif.

Avant de commencer

Vous devez exécuter la procédure de préparation avant d'installer QRadar Risk Manager.

Procédure

1. Sélectionnez normal pour le type de configuration. Sélectionnez **Suivant** et appuyez sur Entrée.
2. Sélectionnez votre zone ou continent pour le fuseau horaire. Sélectionnez **Suivant** et appuyez sur Entrée.
3. Sélectionnez votre région pour le fuseau horaire. Sélectionnez **Suivant** et appuyez sur Entrée.
4. Sélectionnez une version de protocole IP. Sélectionnez **Suivant** et appuyez sur Entrée.
5. Sélectionnez l'interface à spécifier comme interface de gestion. Sélectionnez **Suivant** et appuyez sur Entrée.
6. Entrez vos nom d'hôte, adresse IP, masque de réseau, passerelle, DNS, IP publique et serveur de messagerie. Pour les informations de paramètre de réseau, voir «Informations de paramètre réseau pour IPv4», à la page 6.
7. Sélectionnez **Suivant** et appuyez sur Entrée.
8. Entrez un mot de passe pour configurer le mot de passe root de QRadar Risk Manager.
9. Sélectionnez **Suivant** et appuyez sur Entrée.
10. Entrez à nouveau votre nouveau mot de passe pour le confirmer. Sélectionnez **Terminer** et appuyez sur Entrée. Ce processus dure généralement plusieurs minutes.

Que faire ensuite

Utilisez l'éditeur de déploiement pour ajouter QRadar Risk Manager en tant qu'hôte géré à votre console QRadar.

Ajout de QRadar Risk Manager à la console QRadar

Vous devez ajouter IBM Security QRadar Risk Manager en tant qu'hôte géré à la console IBM Security QRadar.

Avant de commencer

Si vous souhaitez activer la compression, la version minimale de chaque hôte géré doit être la console QRadar 7.1 ou QRadar Risk Manager 7.1.

Pour ajouter un hôte géré sans conversion NAT à votre déploiement lorsque la console a subi une conversion NAT, vous devez faire passer la console QRadar en hôte avec conversion NAT. Vous devez changer la console avant d'ajouter l'hôte géré à votre déploiement. Pour plus d'informations, voir le *guide d'administration d'IBM Security QRadar SIEM*.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL `https://<Adresse IP>`, où <Adresse IP> correspond à l'adresse IP de la console QRadar.
3. Entrez votre nom d'utilisateur et votre mot de passe.
4. Dans l'onglet **Admin**, cliquez sur l'**éditeur de déploiement**.
5. Depuis le menu, sélectionnez **Actions**, puis **Ajouter un hôte géré**.
6. Cliquez sur **Suivant**.
7. Entrez des valeurs pour les paramètres suivants :

Option	Description
Enter the IP of the server or appliance to add	Adresse IP de QRadar Risk Manager.
Enter the root password of the host	Mot de passe root de l'hôte.
Confirm the root password of the host	Confirmation de votre mot de passe.
Host is NATed	Pour activer la conversion d'adresses réseau (NAT) pour un hôte géré, le réseau converti doit utiliser la conversion NAT statique. Pour plus d'informations, voir le *guide d'administration d'IBM Security QRadar SIEM*.
Enable Encryption	Crée un tunnel de chiffrement SSH pour l'hôte. Pour activer le chiffrement entre deux hôtes gérés, chacun de ces hôtes doit exécuter la console QRadar 7.1 ou QRadar Risk Manager 7.1.
Enable Compression	Active la compression de données entre deux hôtes gérés.

8. Sélectionnez l'une des options suivantes :
   - Si vous avez cochez la case **Host is NATed**, vous devez indiquer des valeurs pour les paramètres NAT.

Option	Description
Enter public IP of the server or appliance to add	Adresse IP publique de l'hôte géré. L'hôte géré utilise cette adresse IP pour communiquer avec d'autres hôtes gérés sur différents réseaux utilisant la conversion NAT.
Select NATed network	Réseau que cet hôte géré doit utiliser. Si l'hôte géré se trouve sur le même sous-réseau que la console QRadar, sélectionnez la console du réseau avec conversion NAT. Si l'hôte géré ne se trouve pas sur le même sous-réseau que la console QRadar, sélectionnez l'hôte géré du réseau avec conversion NAT.

   - Si vous n'avez pas coché la case **Host is NATed**, cliquez sur **Suivant**.
9. Cliquez sur **Terminer**. L'exécution de ce processus peut prendre plusieurs minutes. Si votre déploiement inclut des modifications, vous devez déployer tous ces changements.
10. Cliquez sur **Déployer**.

Que faire ensuite

Videz le cache de votre navigateur Web puis connectez-vous à à la console QRadar. L'onglet **Risques** est à présent disponible.

Vidage du cache du navigateur Web

Vous devez vider le cache du navigateur Web pour pouvoir accéder à l'onglet **Risques** de la console QRadar.

Avant de commencer

Vérifiez qu'un seul navigateur Web est ouvert. Si vous avez plusieurs navigateurs ouverts, il est possible que le cache ne soit pas correctement vidé.

Si vous utilisez un navigateur Web Mozilla Firefox, vous également devez vider le cache de votre navigateur Web Microsoft Internet Explorer.

Procédure

1. Ouvrez votre navigateur Web.
2. Videz le cache du navigateur Web. Pour des instructions, reportez-vous à la documentation de votre navigateur Web.

Rôle utilisateur de gestionnaire de risques

Vous devez affecter le rôle utilisateur de gestionnaire de risques (Risk Manager) aux utilisateurs qui ont besoin d'accéder à l'onglet **Risques**.

Un compte utilisateur défini le mot de passe par défaut et l'adresse de courrier électronique d'un utilisateur. Vous devez affecter un rôle utilisateur et un profil de sécurité à chaque nouveau compte utilisateur.

Avant de pouvoir autoriser l'accès à la fonctionnalité IBM Security QRadar Risk Manager à d'autres utilisateurs de votre organisation, vous devez affecter les droits de rôle utilisateur appropriés. Par défaut, la console QRadar fournit un rôle d'administration par défaut qui donne accès à l'ensemble des zones de QRadar Risk Manager.

Pour plus d'informations sur la création et la gestion des rôles utilisateur, voir le *guide d'administration d'IBM Security QRadar SIEM*.

Affectation du rôle utilisateur de gestionnaire de risques

Vous pouvez affecter le rôle utilisateur de gestionnaire de risques (Risk Manager) à des utilisateurs qui ont besoin d'accéder à l'onglet **Risques**.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Configuration système**.
3. Dans le panneau **Gestion des utilisateurs**, cliquez sur l'icône **Rôles utilisateur**.
4. Cliquez sur l'icône **Editer** en regard du rôle utilisateur à éditer.
5. Sélectionnez la case à cocher **Risk Manager**.
6. Cliquez sur **Suivant**. Si vous ajoutez Risk Manager à un rôle utilisateur disposant du droit Log Activity, vous devez définir les sources de journal auxquelles le rôle utilisateur peut accéder. Vous pouvez ajouter un groupe entier de sources de journal en cliquant sur l'icône **Ajouter** dans le panneau **Groupe de sources de journal**. Vous pouvez sélectionner plusieurs sources de journal en maintenant la touche Ctrl enfoncée pendant que vous sélectionnez chaque source de journal à ajouter.

7. Cliquez sur **Retour**.
8. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Dépannage de l'onglet Risques

Vous pouvez traiter les incidents si l'onglet **Risques** ne s'affiche pas correctement ou est inaccessible.

Lorsque l'onglet Risques ne s'affiche pas correctement ou est inaccessible, vous retirez et lisez IBM Security QRadar Risk Manager en tant qu'hôte géré.

Retrait d'un hôte géré

Vous pouvez retirer votre hôte géré IBM Security QRadar Risk Manager de la console IBM Security QRadar pour modifier des paramètres réseau, ou en cas de problème avec l'onglet **Risques**.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL `https://<Adresse IP>`, où <Adresse IP> correspond à l'adresse IP de la console QRadar.
3. Entrez votre nom d'utilisateur et votre mot de passe.

   Pour les informations de connexion par défaut, voir tableau 2, à la page 6.
4. Dans l'onglet **Admin**, cliquez sur l'**éditeur de déploiement**.
5. Cliquez sur l'onglet **SystemView**.
6. Cliquez avec le bouton droit de la souris sur l'hôte géré à supprimer et sélectionnez **Supprimer**. Répétez l'opération pour chaque hôte géré qui n'est pas une console, jusqu'à ce que tous les hôtes soient supprimés.
7. Cliquez sur **Sauvegarder**.
8. Fermez l'éditeur de déploiement.
9. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Lecture de QRadar Risk Manager en tant qu'hôte géré

Vous pouvez lire QRadar Risk Manager en tant qu'hôte géré une fois qu'il a été supprimé.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL `https://<Adresse IP>`, où <Adresse IP> correspond à l'adresse IP de la console QRadar.
3. Entrez votre nom d'utilisateur et votre mot de passe.

   Pour les informations de connexion par défaut, voir tableau 2, à la page 6.
4. Dans l'onglet **Admin**, cliquez sur l'**éditeur de déploiement**.
5. Cliquez sur l'onglet **SystemView**.
6. Dans le menu, sélectionnez **Actions** > **Ajouter un hôte géré**.
7. Cliquez sur **Suivant**.
8. Entrez les valeurs dans la fenêtre Ajouter un nouvel hôte géré.
9. Cliquez sur **Suivant**.
10. Cliquez sur **Terminer**. L'exécution du processus d'ajout de QRadar Risk Manager peut prendre plusieurs minutes.

11. Fermez l'éditeur de déploiement.
12. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Chapitre 3. Installations à l'aide d'une clé USB

Vous pouvez installer des logiciels IBM Security QRadar à l'aide d'une clé USB.

Les installations à l'aide d'une clé USB sont des installations de produit complètes. Vous ne pouvez pas utiliser une clé USB pour mettre à niveau ou appliquer des correctifs de produit. Pour plus d'informations sur l'application des groupes de correctifs, consultez les notes sur l'édition du groupe de correctifs.

Versions prises en charge

Les dispositifs ou systèmes d'exploitation suivants peuvent être utilisés pour créer une clé USB amorçable :

- Un dispositif de QRadar v7.2.1 ou version suivante
- Un système Linux installé avec Red Hat Enterprise Linux 6.4
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2008
- Microsoft Windows 2008R2

Présentation de l'installation

Suivez la procédure ci-après pour installer des logiciels QRadar à partir d'une clé USB :

1. Créez la clé USB amorçable.
2. Installez les logiciels de votre dispositifQRadar.
3. Installez les éditions de maintenance ou les groupes de correctifs produit.

   Consultez les notes sur l'édition pour obtenir des instructions d'installation des groupes de correctifs et des éditions de maintenance.

Création d'une clé USB amorçable avec un dispositif QRadar

Vous pouvez utiliser un dispositif de IBM Security QRadar V7.2.1 ou version suivante pour créer une clé USB amorçable qui peut être utilisée pour installer des logiciels QRadar.

Avant de commencer

Pour pouvoir créer une clé USB amorçable à partir d'un dispositif de QRadar, vous devez avoir accès aux éléments suivants :

- Une clé USB de 2 Go
- Un fichier image ISO de QRadar V7.2.1 ou version suivante
- Un dispositif physique de QRadar

Si votre dispositif QRadar ne dispose pas d'une connexion Internet, vous pouvez télécharger le fichier image ISO de QRadar sur un ordinateur de bureau ou sur un autre dispositif de QRadar doté d'un accès Internet. Vous pouvez ensuite copier le fichier ISO sur le dispositif de QRadar où vous installez les logiciels.

Lorsque vous créez une clé USB amorçable, le contenu de la clé est supprimé.

Procédure

1. Téléchargez le fichier image ISO deQRadar.
   a. Accédez au site Web IBM Support (www.ibm.com/support).
   b. Recherchez le fichier ISO de IBM Security QRadar correspondant à la version du dispositif de QRadar.
   c. Copiez le fichier image ISO dans un répertoire `/tmp` sur votre dispositif QRadar.
2. Avec SSH, connectez-vous à votre système QRadar en tant que superutilisateur.
3. Insérez la clé USB dans le port USB de votre système QRadar.

   Jusqu'à 30 secondes peuvent être nécessaires pour que le système reconnaisse la clé USB.
4. Entrez la commande suivante pour monter l'image ISO :

   `mount -o loop /tmp/<nom de l'image ISO>.iso /media/cdrom`
5. Entrez la commande suivante pour copier le script de création USB de l'image ISO montée dans le répertoire `/tmp`.

   `cp /media/cdrom/post/create-usb-key.py /tmp/`
6. Entrez la commande suivante pour démarrer le script de création USB :

   `/tmp/create-usb-key.py`
7. Appuyez sur la touche `Entrée`.
8. Appuyez sur `1` et entrez le chemin d'accès au fichier ISO. Par exemple,

   `/tmp/<nom de l'image iso>.iso`
9. Appuyez sur `2` et sélectionnez l'unité contenant votre clé USB.
10. Appuyez sur `3` pour créer votre clé USB.

    Le processus d'écriture de l'image ISO sur votre clé USB peut prendre plusieurs minutes. Une fois l'image ISO chargée sur la clé USB, un message de confirmation s'affiche.
11. Appuyez sur `q` pour quitter le script de la clé USB.
12. Retirez la clé USB de votre système QRadar.
13. Pour libérer de l'espace, supprimez le fichier image ISO du système de fichiers `/tmp`.

Que faire ensuite

Si votre connexion au dispositif est une connexion en série, voir Configuration d'une clé USB pour les dispositifs en série uniquement.

Si votre connexion au dispositif est une connexion est de type VGA (clavier et souris), voir Installation de QRadar avec une clé USB.

Création d'une clé USB amorçable sous Microsoft Windows

Vous pouvez utiliser un ordinateur de bureau ou un ordinateur portable sous Microsoft Windows pour créer une clé USB amorçable qui peut être utilisée pour installer des logiciels QRadar.

Avant de commencer

Pour pouvoir créer une clé USB amorçable sous Microsoft Windows, vous devez avoir accès aux éléments suivants :

- Une clé USB de 2 Go
- Un ordinateur de bureau ou un ordinateur portable doté de l'un des systèmes d'exploitation suivants :
  - Windows 7
  - Windows Vista
  - Windows 2008
  - Windows 2008R2

Vous devez télécharger les fichiers suivants du site Web IBM Support (www.ibm.com/support).

- Fichier image ISO 64 bits Red Hat de QRadar V7.2.1 ou version suivante
- Outil CUIK (Create-USB-Install-Key).

Vous devez télécharger les fichiers suivants depuis Internet.

- PeaZip Portable 4.8.1
- SYSLINUX 4.06

Conseil : Effectuez une recherche sur `Peazip Portal v4.8.1` et `Syslinux` sur le Web afin de trouver les fichiers à télécharger.

Lorsque vous créez une clé USB amorçable, le contenu de la clé est supprimé.

Procédure

1. Procédez à l'extraction de l'outil CUIK dans le répertoire`c:\cuik`.
2. Copiez les fichiers `.zip` de PeaZip Portable 4.8.1 et SYSLINUX 4.06 dans le dossier `cuik\deps`.

   Par exemple, `c:\cuik\deps\peazip_portable-4.8.1.WINDOWS.zip` et `c:\cuik\deps\syslinux-4.06.zip`.

   Il n'est pas nécessaire d'extraire les fichiers `.zip`. Ces fichiers doivent uniquement figurer dans le répertoire`cuik/deps`.
3. Insérez la clé USB amorçable dans le port USB de votre ordinateur.
4. Vérifiez que la clé USB est identifiée par un identificateur d'unité et qu'elle est accessible sous Microsoft Windows.
5. Cliquez avec le bouton droit de la souris sur `c:\cuik\cuik.exe`, sélectionnez **Exécuter en tant qu'administrateur** et appuyez sur **Entrée**.
6. Appuyez sur `1`, sélectionnez le fichier ISO deQRadar et cliquez sur **Ouvrir**.
7. Appuyez sur `2` et sélectionnez le nombre correspondant à l'identificateur d'unité affecté à votre clé USB.
8. Appuyez sur `3` pour créer la clé USB.
9. Appuyez sur **Entrée** pour confirmer que vous avez compris que le contenu de la clé USB va être supprimé.
10. Entrez `create` pour créer une clé USB amorçable à partir de l'image ISO. Cette opération peut prendre plusieurs minutes.
11. Appuyez sur **Entrée**, puis entrez `q` pour quitter l'outil Create_USB_Install_Key.
12. Retirez en toute sécurité la clé USB de votre ordinateur.

Que faire ensuite

Si votre connexion au dispositif est une connexion en série, voir Configuration d'une clé USB pour les dispositifs en série uniquement.

Si votre connexion au dispositif est une connexion est de type VGA (clavier et souris), voir Installation de QRadar avec une clé USB.

Création d'une clé USB amorçable avec Red Hat Linux

Vous pouvez utiliser un ordinateur de bureau ou un ordinateur portable Linux avec Red Hat v6.3 pour créer une clé USB amorçable qui peut être utilisée pour installer des logiciels IBM Security QRadar.

Avant de commencer

Pour pouvoir créer une clé USB amorçable avec un système Linux, vous devez avoir accès aux éléments suivants :

- Une clé USB de 2 Go
- Un fichier image ISO de QRadar V7.2.1 ou version suivante
- Un système Linux sur lequel sont installés les logiciels suivants :
  - Red Hat 6.4
  - Python 6.2 ou version suivante

Lorsque vous créez une clé USB amorçable, le contenu de la clé est supprimé.

Procédure

1. Téléchargez le fichier image ISO deQRadar.
   a. Accédez au site Web IBM Support (www.ibm.com/support).
   b. Localisez le fichier ISO de IBM Security QRadar ISO.
   c. Copiez le fichier image ISO dans un répertoire `/tmp` sur votre dispositif QRadar.
2. Mettez à jour votre système Linux avec les packages ci-après.
   - syslinux
   - mtools
   - dosfstools
   - parted

   Pour plus d'informations sur le gestionnaire de package spécifique à votre système Linux, consultez la documentation du fournisseur.
3. Connectez-vous à votre système QRadar en tant que superutilisateur.
4. Insérez la clé USB dans le port USB avant de votre système.

   Jusqu'à 30 secondes peuvent être nécessaires pour que le système reconnaisse la clé USB.
5. Entrez la commande suivante pour monter l'image ISO :

   ```
   mount -o loop /tmp/<nom de l'image ISO>.iso /media/cdrom
   ```
6. Entrez la commande suivante pour copier le script de création USB de l'image ISO montée dans le répertoire `/tmp`.

   ```
   cp /media/cdrom/post/create-usb-key.py /tmp/
   ```
7. Entrez la commande suivante pour démarrer le script de création USB :

   ```
   /tmp/create-usb-key.py
   ```

8. Appuyez sur la touche Entrée.
9. Appuyez sur 1 et entrez le chemin d'accès au fichier ISO. Par exemple, /tmp/Rhe664QRadar7_2_4_<*build*>.iso
10. Appuyez sur 2 et sélectionnez l'unité contenant votre clé USB.
11. Appuyez sur 3 pour créer votre clé USB.

    Le processus d'écriture de l'image ISO sur votre clé USB peut prendre plusieurs minutes. Une fois l'image ISO chargée sur la clé USB, un message de confirmation s'affiche.
12. Appuyez sur q pour quitter le script de la clé USB.
13. Retirez la clé USB de votre système.

Que faire ensuite

Si votre connexion au dispositif est une connexion en série, voir Configuration d'une clé USB pour les dispositifs en série uniquement.

Si votre connexion au dispositif est une connexion est de type VGA (clavier et souris), voir Installation de QRadar avec une clé USB.

Configuration d'une clé USB pour les dispositifs en série uniquement

Vous devez effectuer une étape de configuration supplémentaire avant d'utiliser la clé USB amorçable pour installer des logiciels QRadar sur les dispositifs en série uniquement.

Pourquoi et quand exécuter cette tâche

Cette procédure n'est pas obligatoire si vous avez connecté un clavier et une souris à votre dispositif.

Procédure

1. Insérez la clé USB amorçable dans le port USB de votre dispositif.
2. Sur votre clé USB, recherchez le fichier syslinux.cfg.
3. Editez le fichier de configuration syslinux afin de remplacer l'installation par défaut default linux par default serial.
4. Sauvegarder les modifications dans le fichier de configuration syslinux.

Que faire ensuite

Vous être maintenant prêt pour l'installation de QRadar avec la clé USB.

Installation de QRadar à l'aide d'une clé USB

Suivez la procédure ci-après pour installer QRadar depuis une clé USB amorçable.

Avant de commencer

Vous devez créer la clé USB amorçable avant de l'utiliser pour installer des logiciels QRadar.

Pourquoi et quand exécuter cette tâche

Cette procédure fournit des conseils généraux sur la manière d'utiliser une clé USB amorçable pour l'installation de logiciels QRadar.

Le processus d'installation complet est présenté en détail dans le guide d'installation du produit.

Procédure

1. Installez tout le matériel nécessaire.
2. Sélectionnez l'une des options suivantes :
   - Connecter un ordinateur portable au port série situé à l'arrière du dispositif.
   - Connecter un clavier et un moniteur à leurs ports respectifs.
3. Insérez la clé USB amorçable dans le port USB de votre dispositif.
4. Redémarrez le dispositif.

   La plupart des dispositifs peuvent s'amorcer depuis une clé USB par défaut. Si vous installez les logiciels QRadar sur votre propre matériel, vous devrez peut-être définir l'ordre d'amorçage des unités afin de définir la clé USB comme prioritaire.

   Une fois le dispositif démarré, la clé USB prépare le dispositif pour l'installation. Ce processus peut prendre jusqu'à une heure.
5. Lorsque le menu **Red Hat Enterprise Linux** s'affiche, sélectionnez l'une des options suivantes :
   - Si vous avez connecté un clavier et un moniteur, sélectionnez **Install or upgrade using VGA console**.
   - Si vous avez connecté un ordinateur portable avec une connexion série, sélectionnez **Install or upgrade using Serial console**.
6. Entrez `SETUP` pour commencer l'installation.
7. Lorsque l'invite de connexion s'affiche, entrez `root` pour vous connecter au système en tant que superutilisateur.

   Le nom d'utilisateur différencie les majuscules des minuscules.
8. Appuyez sur **Enter** et suivez les invites pour installer QRadar.

   Le processus d'installation complet est présenté en détail dans le guide d'installation du produit.

Chapitre 4. Réinstallation d'IBM Security QRadar Risk Manager depuis la partition de récupération

Lorsque vous réinstallez IBM Security QRadar Risk Manager depuis la console IBM Security QRadar ISO sur la partition de récupération, la configuration usine par défaut de votre système est restaurée. Cela signifie que votre configuration et les fichiers de données en cours sont écrasés.

Ces informations s'appliquent aux nouvelles installations ou aux mises à niveau de QRadar Risk Manager à partir de nouvelles installations de QRadar Risk Manager sur des dispositifs QRadar Risk Manager. Lorsque vous installez QRadar Risk Manager, le programme d'installation (console QRadar ISO) est copié sur la partition de récupération. Cette partition permet de réinstaller QRadar Risk Manager, en restaurant les paramètres par défaut définis en d'usine de QRadar Risk Manager.

Remarque : Si vous mettez à niveau votre logiciel après avoir installé QRadar Risk Manager, le fichier ISO est remplacé par la version plus récente.

Lorsque vous réamorcez votre dispositif QRadar Risk Manager, vous avez la possibilité de réinstaller le logiciel. La console QRadar et QRadar Risk Manager utilisant le même fichier d'installation ISO, le nom ISO de QRadar console s'affiche.

Si vous ne répondez pas à l'invite sous 5 secondes, le système effectue un redémarrage normal et conserve vos fichiers de configuration et de données. Si vous choisissez de réinstaller la console QRadar ISO, un message d'avertissement s'affiche et vous devez confirmer que vous souhaitez réinstaller le logiciel. Après confirmation de votre part, le programme d'installation s'exécute et vous pouvez suivre les invites via le processus d'installation.

En cas de défaillance de disque dur, vous ne pouvez pas effectuer de réinstallation à partir de la partition de récupération car celle-ci n'est plus disponible. Dans ce cas de figure, contactez le service clients pour une assistance.

Réinstallation de QRadar Risk Manager via la réinstallation de la version usine

Vous pouvez réamorcer et réinstaller votre dispositif QRadar Risk Manager en utilisant l'option de réinstallation des valeurs usine.

Avant de commencer

Assurez-vous que vous disposez de la clé d'activation, chaîne alphanumérique de 24 chiffres répartis en quatre groupes de chiffres qui vous est fournie par IBM. Où trouver la clé :

- Imprimée sur un autocollant apposé sur votre dispositif.
- Fournie avec le bordereau de marchandises ; les dispositifs y figurent avec leurs clés associées.

Afin d'éviter toute erreur de frappe, la lettre I et le nombre 1 (un) sont traités de manière identique, tout comme la lettre O et le nombre 0 (zéro).

Si vous ne disposez pas d'une clé d'activation pour votre dispositif QRadar Risk Manager, prenez contact avec le service clients (http://www.ibm.com/support).

Les clés d'activation logicielles ne nécessitent pas de numéro de série.

Procédure

1. Réamorcez votre dispositif QRadar Risk Manager.
2. Sélectionnez l'option permettant de **réinstaller la version usine**.
3. Entrez `flatten` pour continuer. Le disque dur est partitionné et reformaté, le système d'exploitation est installé, puis qradar Risk Manager est réinstallé. Vous devez attendre la fin d'exécution du processus de mise à plat. Ce processus peut prendre plusieurs minutes selon votre système.
4. Tapez `SETUP`.
5. Connectez-vous à QRadar Risk Manager en tant qu'utilisateur root.
6. Lisez les informations à l'écran. Appuyez sur la barre d'espacement pour passer à l'écran suivant, jusqu'à ce que vous parveniez à la fin du document. Tapez `yes` pour accepter le contrat, puis appuyez sur Entrée.
7. Entrez votre clé d'activation et appuyez sur Entrée.
8. Sélectionnez **normal** pour le type de configuration. Sélectionnez **Suivant** et appuyez sur Entrée.
9. Sélectionnez votre zone ou continent pour le fuseau horaire. Sélectionnez **Suivant** et appuyez sur Entrée.
10. Sélectionnez votre région pour le fuseau horaire. Sélectionnez **Suivant** et appuyez sur Entrée.
11. Sélectionnez une version de protocole IP. Sélectionnez **Suivant** et appuyez sur Entrée.
12. Sélectionnez l'interface à spécifier comme interface de gestion. Sélectionnez **Suivant** et appuyez sur Entrée.
13. Entrez les informations de nom d'hôte, adresse IP, masque de réseau, passerelle, DNS, IP publique et serveur de messagerie. Pour les informations relatives au réseau, voir «Informations de paramètre réseau pour IPv4», à la page 6.
14. Entrez votre mot de passe pour configurer le mot de passe root de QRadar Risk Manager.
15. Sélectionnez **Suivant** et appuyez sur Entrée.
16. Entrez à nouveau votre nouveau mot de passe pour le confirmer. Sélectionnez **Terminer** et appuyez sur Entrée. Ce processus dure généralement plusieurs minutes.
17. Appuyez sur Entrée pour sélectionner OK.
18. Appuyez sur Entrée pour sélectionner OK.

Que faire ensuite

Utilisez l'éditeur de déploiement pour ajouter QRadar Risk Manager en tant qu'hôte géré à votre console QRadar.

Chapitre 5. Modification des paramètres réseau

Vous pouvez changer les paramètres réseau d'un dispositif IBM Security QRadar Risk Manager qui est connecté à une console IBM Security QRadar.

Si vous avez besoin de changer les paramètres réseau, vous devez exécuter les tâches ci-après dans l'ordre indiqué :

1. Retrait de QRadar Risk Manager en tant qu'hôte géré.
2. Modification des paramètres réseau.
3. Lecture de QRadar Risk Manager en tant qu'hôte géré.

Retrait d'un hôte géré

Vous pouvez retirer votre hôte géré IBM Security QRadar Risk Manager de la console IBM Security QRadar pour modifier des paramètres réseau, ou en cas de problème avec l'onglet **Risques**.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL `https://<Adresse IP>`, où <Adresse IP> correspond à l'adresse IP de la console QRadar.
3. Entrez votre nom d'utilisateur et votre mot de passe.

   Pour les informations de connexion par défaut, voir tableau 2, à la page 6.
4. Dans l'onglet **Admin**, cliquez sur l'**éditeur de déploiement**.
5. Cliquez sur l'onglet **SystemView**.
6. Cliquez avec le bouton droit de la souris sur l'hôte géré à supprimer et sélectionnez **Supprimer**. Répétez l'opération pour chaque hôte géré qui n'est pas une console, jusqu'à ce que tous les hôtes soient supprimés.
7. Cliquez sur **Sauvegarder**.
8. Fermez l'éditeur de déploiement.
9. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Modification des paramètres réseau

Vous pouvez changer les paramètres réseau d'un dispositif IBM Security QRadar Risk Manager qui est connecté à une console IBM Security QRadar.

Avant de commencer

Vous devez retirer l'hôte géré QRadar Risk Manager de la console QRadar avant de procéder aux modifications de paramètres réseau.

Procédure

1. A l'aide de Secure Shell (SSH), connectez-vous à QRadar Risk Manager en tan qu'utilisateur racine (root).
2. Entrez la commande `qchange_netsetup`.

3. Sélectionnez une version de protocole IP. Sélectionnez **Suivant** et appuyez sur Entrée. Selon votre configuration matérielle, la fenêtre affiche jusqu'à quatre interface. Chaque interface comportant une liaison physique est signalée par un symbole plus (+).
4. Sélectionnez l'interface à spécifier comme interface de gestion. Sélectionnez **Suivant** et appuyez sur Entrée.
5. Entrez les informations de nom d'hôte, adresse IP, masque de réseau, passerelle, DNS, IP publique et serveur de messagerie. Pour les informations relatives au réseau, voir «Informations de paramètre réseau pour IPv4», à la page 6.
6. Entrez votre mot de passe pour configurer le mot de passe root de QRadar Risk Manager.
7. Sélectionnez **Suivant** et appuyez sur Entrée.
8. Entrez à nouveau votre nouveau mot de passe pour le confirmer. Sélectionnez **Terminer** et appuyez sur Entrée. Ce processus dure généralement plusieurs minutes.

Lecture de QRadar Risk Manager en tant qu'hôte géré

Vous pouvez lire QRadar Risk Manager en tant qu'hôte géré une fois qu'il a été supprimé.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL `https://<Adresse IP>`, où <Adresse IP> correspond à l'adresse IP de la console QRadar.
3. Entrez votre nom d'utilisateur et votre mot de passe.

   Pour les informations de connexion par défaut, voir tableau 2, à la page 6.
4. Dans l'onglet **Admin**, cliquez sur l'**éditeur de déploiement**.
5. Cliquez sur l'onglet **SystemView**.
6. Dans le menu, sélectionnez **Actions** > **Ajouter un hôte géré**.
7. Cliquez sur **Suivant**.
8. Entrez les valeurs dans la fenêtre Ajouter un nouvel hôte géré.
9. Cliquez sur **Suivant**.
10. Cliquez sur **Terminer**. L'exécution du processus d'ajout de QRadar Risk Manager peut prendre plusieurs minutes.
11. Fermez l'éditeur de déploiement.
12. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Chapitre 6. Sauvegarde et restauration des données

Vous pouvez utiliser un script d'interface de ligne de commande pour sauvegarder les données stockées sur les hôtes gérés par la console IBM Security QRadar.

Vous pouvez utiliser le script de l'interface de ligne de commande pour restaurer IBM Security QRadar Risk Manager après un incident données ou matériel sur le dispositif.

Un script de sauvegarde est inclus dans QRadar Risk Manager et il peut être planifié à l'aide de crontab. Le script crée automatiquement une archive quotidienne de QRadar Risk Manager data à 3 heures du matin. Par défaut, QRadar Risk Manager conserve les cinq dernières sauvegardes. Si vous disposez d'un stockage réseau ou connecté, vous devez créer un travail cron pour copier les archives de de sauvegarde de QRadar Risk dans un emplacement de stockage réseau.

L'archive de sauvegarde inclut les données suivantes :

- Configurations d'unité QRadar Risk Manager
- Données de connexion
- Données topologiques
- Questions Policy Monitor
- Tables de base de données QRadar Risk Manager

Pour plus d'informations sur la migration depuis QRadar Risk Manager Maintenance version 5 vers la version en cours, consultez le manuel *IBM Security QRadar Risk Manager Migration Guide*.

Prérequis à la sauvegarde et la restauration de données

Vous devez comprendre comment les données sont sauvegardées, stockées et archivées avant de sauvegarder et restaurer vos données.

Emplacement de sauvegarde des données

Les données sont sauvegardées dans le répertoire local `/Store/qrm_backups`. Votre système peut inclure le montage `/store/backup` à partir d'un service SAN ou NAS externe. Les services externes offrent une conservation hors ligne sur le long terme des données. Un stockage à long terme peut être nécessaire pour le respect des règles de conformité, par exemple les normes PCI (Payment Card Industry).

Version de dispositif

La version du dispositif ayant servi à la création de la sauvegarde en archive est stockée. Une sauvegarde peut uniquement être restaurée sur un dispositif QRadar Risk Manager s'ils sont de la même version.

Fréquence de sauvegarde des données et informations d'archivage

Des sauvegardes de données quotidiennes sont créées à 3h00. Seuls les cinq derniers fichiers de sauvegarde sont stockés. Une archive de sauvegarde est créée s'il y a suffisamment d'espace libre dans QRadar Risk Manager.

Format des fichiers de sauvegarde

Utilisez le format suivant pour sauvegarder des fichiers de sauvegarde :
`backup-<date cible>-<horodatage>.tgz`

Où :

`<date cible>` correspond à la date de création du fichier de sauvegarde.

La date cible est au format suivant : `<jour>_<mois>_<année>`. `<horodatage>` correspond à l'heure de création du fichier de sauvegarde. L'horodatage est au format suivant : `<heure>_<minutes>_<secondes>`.

Sauvegarde de vos données

La sauvegarde automatique a lieu chaque jour, à 3h00, mais vous pouvez démarrer manuellement le processus de sauvegarde.

Procédure

1. A l'aide de SSH, connectez-vous à votre console QRadar en tant que superutilisateur.
2. A l'aide de SSH depuis la console QRadar, connectez-vous à QRadar Risk Manager en tant que superutilisateur.
3. Démarrez une sauvegarde de QRadar Risk Manager en entrant `/opt/qradar/bin/dbmaint/risk_manager_backup.sh`

Résultats

Le démarrage du script utilisé pour lancer le processus de sauvegarde peut prendre plusieurs minutes.

Une fois que le script a terminé la sauvegarde, le message suivant s'affiche :

```
Tue Sep 11 10:14:41 EDT 2012
- Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Restauration de données

Vous pouvez utiliser un script de restauration pour restaurer des données à partir d'une sauvegarde QRadar Risk Manager.

Avant de commencer

Le dispositif QRadar Risk Manager et l'archive de sauvegarde doivent être à la même version de QRadar Risk Manager. Si le script détecte une différence de version entre l'archive et l'hôte géré par QRadar Risk Manager, une erreur s'affiche.

Pourquoi et quand exécuter cette tâche

Utilisez le script de restauration pour indiquer l'archive restaurée dans QRadar Risk Manager. Ce processus implique que vous arrêtiez les services dans QRadar Risk Manager. L'arrêt des services déconnecté tous les utilisateurs QRadar Risk Manager et arrête plusieurs processus.

Le tableau suivant répertorie les paramètres que vous pouvez utiliser pour restaurer une archive de sauvegarde.

Tableau 3. Paramètres utilisés pour restaurer une archive de sauvegarde dans QRadar Risk Manager

Option	Description
-f	Remplace des données QRadar Risk Manager existantes sur votre système par les données du fichier de restauration. La sélection de ce paramètre permet au script de remplacer toute configuration d'unité existant dans la gestion de sources de configuration par les configurations d'unité du fichier de sauvegarde.
-w	Ne pas supprimer de répertoires avant de restaurer les données QRadar Risk Manager.
-h	Aide du script de restauration.

Procédure

1. A l'aide de SSH, connectez-vous à votre console QRadar SIEM en tant que superutilisateur.
2. A l'aide de SSH depuis la console QRadar SIEM, connectez-vous à QRadar Risk Manager en tant que superutilisateur.
3. Arrêtez hostcontext en entrant `service hostcontext stop`.
4. Entrez la commande suivante pour restaurer une archive de sauvegarde dans QRadar Risk Manager : `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>`. Où `<backup>` est l'archive QRadar Risk Manager que vous voulez restaurer.

   Par exemple, backup-2012-09-11-10-14-39.tgz.
5. Démarrez hostcontext en entrant `service hostcontext start`.

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 :

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

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

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

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

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

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

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

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

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corporation aux États-Unis et/ou dans d'autres pays. Si ces marques et d'autres marques d'IBM sont accompagnées d'un symbole de marque (® ou ™), ces symboles signalent des marques d'IBM aux Etats-Unis à la date de publication de ce document. Ces marques peuvent également exister et éventuellement avoir été enregistrées dans d'autres pays. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Adobe et Acrobat ainsi que toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Java et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

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

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

Remarques sur les règles de confidentialité

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

Selon les configurations déployées, cette Offre logicielle peut utiliser des cookies de session qui collectent chaque ID de session à des fins de gestion de la session et

d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

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

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

Index