IBM Security QRadar Risk Manager
Version 7.2.6

Guide d'utilisation

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations fournies à la section «Remarques», à la page 31.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.6 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 être utilisées avec IBM® Security QRadar Risk Manager. QRadar Risk Manager est un dispositif utilisé pour surveiller des configurations d'unités, simuler des modifications apportées à votre environnement réseau, et hiérarchiser les risques et vulnérabilités dans votre réseau.

Ce guide contient les instructions d'installation de QRadar Risk Manager et d'ajout de QRadar Risk Manager en tant que hôte géré sur une console IBM Security QRadar SIEM Console.

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

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

Contacter le service clients

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

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit

ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

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. Préparation à l'installation de IBM Security QRadar Risk Manager

Vous installez un appareil IBM Security QRadar Risk Manager en tant qu'hôte géré sur IBM Security QRadar SIEM Console. Un seul QRadar Risk Manager peut exister sur QRadar Console.

QRadar Console et QRadar Risk Manager utiliser le même processus d'installation et la même image ISO. Une fois QRadar Console et QRadar Risk Manager installés, ajoutez QRadar Risk Manager en tant que hôte géré à l'aide de de **Gestion du système et de la licence** dans l'onglet **Admin**. Un appareil QRadar Risk Manager est préinstallé avec le logiciel QRadar Risk Manager et un système d'exploitation Red Hat Enterprise Linux.

Chapitre 2. Avant de procéder à l'installation

Vous devez terminer le processus d'installation d'IBM Security QRadar SIEM Console 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 exigences matérielles et logicielles, voir *IBM Security QRadar SIEM Administration Guide*.

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-feu entre IBM Security QRadar SIEM Console et IBM Security QRadar Risk Manager doivent autoriser le trafic sur certains ports.

Vérifiez que tout pare-feu situé entre la console QRadar SIEM Console 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 IBM Security QRadar Risk Manager

Il est important de connaître les fonctions qui ne sont pas prises en charge par 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

Chapitre 3. Configuration matérielle supplémentaire

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

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

- Moniteur et clavier
- Alimentation de secours (UPS)

Protégéz vos installations QRadar Risk Manager, chargées de stocker vos données à l'aide d'une alimentation de secours (UPS). Celle-ci permet de préserver vos données QRadar Risk Manager, telles que celles stockées sur vos consoles, vos processeurs d'événement et Collecteurs QRadar QFlow, pendant une panne d'alimentation.

Chapitre 4. 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 :

- Java™ Runtime Environment
- Adobe Flash, version 10 ou supérieure

Chapitre 5. 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	38.0 Extended Support Release
Microsoft Internet Explorer 32 bits, avec mode document et mode navigateur activés	10.0 11.0
Google Chrome	Version 46

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 **Document Mode** et sélectionnez **Internet Explorer standards** pour votre version d'Internet Explorer.

Chapitre 6. Installation des dispositifs IBM Security QRadar Risk Manager

Un déploiement IBM Security QRadar Risk Manager comprend un dispositif IBM Security QRadar SIEM Console et 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'une clé d'activation. La clé d'activation se caractérise par une chaîne alphanumérique composée de 24 caractères, 4 parties que vous recevez via IBM. Où trouver la clé d'activation :

- Elle peut être imprimée sur un autocollant apposé sur votre dispositif.
- Elle peut être incluse avec le bon de livraison sur lequel tous les dispositifs sont répertoriés avec les 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 Service clients (Support Portal) (www.ibm.com/support/).

Pour des informations sur votre dispositif, voir *IBM Security QRadar Hardware Installation Guide*.

Procédure

1. Connectez un clavier et un moniteur à leurs ports respectifs.
2. Mettez sous tension le système et connectez-vous. Le nom d'utilisateur, sensible à la casse, est superutilisateur.
3. Appuyez sur la touche **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 puis appuyez sur Entrée.

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

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

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

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

Informations de connexion	**Valeur par défaut**
URL	`https://<Adresse IP>`, où*<Adresse IP>* est l'adresse IP de la QRadar Console.
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

Informations de réseau pour Internet Protocol version 4 (IPv4) Un réglage du réseau est nécessaire 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 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 en utilisant les services NAT (Network Address Translation) sur votre réseau ou dans 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 après la préparation de votre appareil.

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 les informations concernant vos nom d'hôte, adresse IP, masque de sous-réseau, passerelle, DNS principal, DNS secondaire, adresse IP publique, et serveur de messagerie. Pour les informations de paramètre de réseau, voir «Informations de paramètre réseau pour IPv4», à la page 12.
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.

Ajout de IBM Security QRadar Risk Manager à IBM Security QRadar SIEM Console

Vous pouvez ajouter IBM Security QRadar Risk Manager en tant qu'hôte géré à IBM Security QRadar SIEM Console.

Avant de commencer

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

Pour ajouter un hôte géré sans conversion d'adresses réseau à votre déploiement disposant de la console avec conversion d'adresses, vous devez remplacer QRadar Console par un hôte avec conversion d'adresses réseau. Vous devez changer la console avant d'ajouter l'hôte géré à votre déploiement. Pour plus d'informations, voir *IBM Security QRadar SIEM Administration Guide*.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL, `https://<Adresse_IP>`, où *<Adresse_IP>* représente l'adresse IP de la console QRadar Console.
3. Entrez votre nom d'utilisateur et votre mot de passe.
4. Cliquez sur l'onglet **Admin**.
5. Dans le panneau Configuration système, cliquez sur **Gestion du système et de la licence**.
6. Dans la fenêtre Gestion du système et de la licence, cliquez sur **Actions de déploiement**, puis sélectionnez **Ajouter l'hôte**.
7. Cliquez sur **Suivant**.
8. Entrez des valeurs pour les paramètres suivants :

Option	Description
IP hôte	Adresse IP de QRadar Risk Manager.
Mot de passe hôte	Mot de passe root de l'hôte.
Confirmer le mot de passe de l'hôte :	Confirmation de votre mot de passe.
Chiffrer les connexions hôtes	Crée un tunnel de chiffrement SSH pour l'hôte. Pour activer le chiffrement entre deux hôtes gérés, chaque hôte géré doit exécuter QRadar Console version 7.1 ou QRadar Risk Manager version 7.1.

Option	Description
Compression de chiffrement	Permets de chiffrer la compression de données entre deux hôtés gérés.
conversion d'adresses réseau (NAT)	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 *IBM Security QRadar SIEM Administration Guide*.

9. Si vous cochez la case **Conversion d'adresses réseau**, alors vous devez entrer les valeurs des paramètres de conversion d'adresses réseau :

Option	Description
Groupe NAT	Réseau que cet hôte géré doit utiliser. Si l'hôte géré se trouve sur le même sous-réseau que QRadar Console, sélectionnez la console du réseau en NAT. Si l'hôte géré ne se trouve pas sur le même sous-réseau que QRadar Console, sélectionner l'hôte géré du réseau avec conversion d'adresses réseau.
Adresse IP publique	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.

10. Cliquez sur **Ajouter**. L'exécution de ce processus peut prendre plusieurs minutes. Si votre déploiement inclut des modifications, vous devez déployer tous ces changements.
11. Depuis l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.

Que faire ensuite

Videz le cache de votre navigateur Web puis connectez-vous à à la console QRadar Console. 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 IBM Security QRadar SIEM Console.

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.

Chapitre 7. 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 d'autoriser les utilisateurs de votre organisation à accéder aux fonctions IBM Security QRadar Risk Manager, vous devez affecter les droits de rôles utilisateur appropriés. Par défaut, la console QRadar Console 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 de rôles utilisateurs, voir *IBM Security QRadar SIEM Administration Guide*.

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

Chapitre 8. 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 ajoutez à nouveau 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 SIEM Console pour modifier des paramètres réseau, ou en cas de problème avec l'onglet **Risques**.

Procédure

1. Connectez-vous à QRadar Console en tant qu'administrateur :

   `https://`*`Adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe est le mot de passe du compte de l'utilisateur root qui a été entré lors de l'installation.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. À partir de la table d'hôte, cliquez sur l'hôte QRadar Risk Manager que vous souhaitez supprimer et cliquez sur **Actions de déploiement** > **Supprimer l'hôte**.
5. Dans la barre de menu de l'onglet **Admin**, cliquez sur **Déployer les changements**.
6. Actualisez votre navigateur Web.

Chapitre 9. Nouvel ajout de IBM Security QRadar Risk Manager en tant qu'hôte géré

Vous pouvez ajouter à nouveau IBM Security QRadar Risk Manager en tant qu'hôte géré une fois qu'il a été supprimé.

Procédure

1. Dans l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Ajouter un hôte**.
2. Entrez l'adresse IP de l'hôte et le mot de passe.
3. Cliquez sur **Ajouter**.

   Vous devez attendre quelques minutes que l'hôte géré soit ajouté.
4. Fermez la fenêtre Gestion du système et de la licence.
5. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
6. Cliquez sur **OK**.

Chapitre 10. 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 SIEMIBM Security QRadar SIEM Console 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 mises à niveau QRadar Risk Manager à partir d'une nouvelle instance QRadar Risk Manager sur des appareils QRadar Risk Manager. Lorsque vous installez QRadar Risk Manager, le programme d'installation (QRadar Console ISO) est copié dans 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 Console 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 QRadar Console 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 IBM Security QRadar Risk Manager via la réinstallation de la version usine

Vous pouvez redémarrer et réinstaller votre appareil IBM Security QRadar Risk Manager en utilisant l'option d'installation d'usine.

Avant de commencer

Vérifiez que vous possédez votre clé d'activation représentant une chaîne alphanumérique composée de 24 caractères, 4 parties que vous recevez via IBM. Vous pouvez trouver la clé dans ces lieux :

- Elle peut être imprimée sur un autocollant apposé sur votre dispositif.
- Elle peut être incluse avec le bon de livraison sur lequel tous les dispositifs sont répertoriés avec les 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 Service clients (Support Portal) (www.ibm.com/support/).

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

Procédure

1. Redémarrez votre appareil 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 comme 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. Suivez les instructions de l'assistant.

   Ce processus dure généralement plusieurs minutes.
9. Appuyez sur `Entrée` pour sélectionner `OK`.
10. Appuyez sur `Entrée` pour sélectionner `OK`.

Chapitre 11. Modification des paramètres réseau

Vous pouvez modifier les paramètres réseau d'un appareil IBM Security QRadar Risk Manager qui est connecté à IBM Security QRadar SIEM Console.

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. Nouvel ajout de QRadar Risk Manager en tant que hôte géré..

Retrait d'un hôte géré

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

Procédure

1. Connectez-vous à QRadar Console en tant qu'administrateur :

   `https://`*`Adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe est le mot de passe du compte de l'utilisateur root qui a été entré lors de l'installation.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. À partir de la table d'hôte, cliquez sur l'hôte QRadar Risk Manager que vous souhaitez supprimer et cliquez sur **Actions de déploiement** > **Supprimer l'hôte**.
5. Dans la barre de menu de l'onglet **Admin**, cliquez sur **Déployer les changements**.
6. Actualisez votre navigateur Web.

Modification des paramètres réseau

Vous pouvez modifier les paramètres réseau d'un appareil IBM Security QRadar Risk Manager qui est connecté à IBM Security QRadar SIEM Console.

Avant de commencer

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

Procédure

1. En utilisant Secure Shell (SSH), connectez-vous à QRadar Risk Manager en tan qu'utilisateur 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 concernant vos nom d'hôte, adresse IP, masque de sous-réseau, passerelle, DNS principal, DNS secondaire, adresse IP publique, et serveur de messagerie. Pour les informations relatives au réseau, voir «Informations de paramètre réseau pour IPv4», à la page 12.
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.

Nouvel ajout de IBM Security QRadar Risk Manager en tant qu'hôte géré

Vous pouvez ajouter à nouveau IBM Security QRadar Risk Manager en tant qu'hôte géré une fois qu'il a été supprimé.

Procédure

1. Dans l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Ajouter un hôte**.
2. Entrez l'adresse IP de l'hôte et le mot de passe.
3. Cliquez sur **Ajouter**.

   Vous devez attendre quelques minutes que l'hôte géré soit ajouté.
4. Fermez la fenêtre Gestion du système et de la licence.
5. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
6. Cliquez sur **OK**.

Chapitre 12. 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 IBM Security QRadar SIEM Console.

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 données QRadar Risk Manager 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 Manager dans un emplacement de stockage réseau.

L'archive de sauvegarde inclut les données suivantes :

- Configuration 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 permettent de conserver les données hors ligne sur le long terme. 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 suvegarde peut être uniquement restaurée dans un dispositif IBM Security QRadar Risk Manager si la version est identique.

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>` représente 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 se présente de la façon suivante : `<heure>_<minute>_<seconde>`.

Sauvegarde de vos données

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

Procédure

1. En utilisant Secure Shell (SSH), connectez-vous à votre console IBM Security QRadar SIEM Console en tan qu'utilisateur root.
2. Grâce à SSH à partir de la console QRadar Console, connectez-vous à QRadar Risk Manager en tant que superutilisateur.
3. Démarrez une sauvegarde de QRadar Risk Manager en entrant la commande suivante :

   ```
   /opt/qradar/bin/dbmaint/risk_manager_backup.sh
   ```

Résultats

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

Le message suivant illustre le résultat affiché, une fois que le script termine la sauvegarde :

```
Fri Sep 11 10:14:41 EDT 2015
- Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2015-09-11-10-14-39.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. En utilisant Secure Shell (SSH), connectez-vous à votre console IBM Security QRadar SIEM Console en tan qu'utilisateur root.
2. Grâce à SSH à partir de la console QRadar SIEM Console, connectez-vous à QRadar Risk Manager en tant que superutilisateur.
3. Arrêtez `hostcontext` en saisissant `service hostcontext stop`.
4. Entrez la commande suivante pour restaurer une archive de sauvegarde vers QRadar Risk Manager :

   `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>`.

   où `<backup>` représente QRadar Risk Manager archive que vous souhaitez restaurer.

   Par exemple, `backup-2012-09-11-10-14-39.tgz`.
5. Démarrez `hostcontext` en saisissant `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
USA

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.comsont des marques d'International Business Machines déposées 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.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated 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.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

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

Remarques sur les règles de confidentialité

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

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

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres

personnes via des cookies et d'autres technologies, vous devez vous renseigner sur l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

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