IBM Security QRadar
Version 7.2.8

Guide d'installation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 77.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.8 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 des installations de QRadar

Les dispositifs IBM® Security QRadar sont pré-installés avec des logiciels et le système d'exploitation Red Hat Enterprise Linux. Vous pouvez également installer le logiciel QRadar sur votre propre matériel.

Nous vous remercions d'avoir fait confiance à IBM pour commander votre dispositif ! Il est vivement recommandé de lui appliquer le dernier niveau de maintenance pour obtenir les meilleurs résultats. Rendez-vous sur le site IBM Fix Central (http://www.ibm.com/support/fixcentral) pour déterminer le correctif recommandé le plus récent pour votre produit.

Pour installer ou restaurer un système haute disponibilité (HD), voir *IBM Security QRadar High Availability Guide*.

Utilisateurs concernés

Les administrateurs de réseau qui sont responsables de l'installation et de la configuration des systèmes QRadar doivent avoir une bonne connaissance des concepts de sécurité réseau et du système d'exploitation Linux.

Documentation technique

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

Pour savoir comment accéder à d'autres documents techniques dans la bibliothèque produit QRadar, voir la note technique Accessing IBM Security Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

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

Instructions relatives aux bonnes pratiques de sécurité

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

L'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.

QRadar version 7.2.8 - Nouveautés pour les responsables de l'installation

IBM Security QRadar version 7.2.8 est livré avec IBM Security Master Console et ses performances ont été améliorées.

IBM Security Master Console désormais fourni avec QRadar

Master Console est automatiquement installé lors de l'installation d'IBM Security QRadar version 7.2.8 avec la clé d'activation 8500 (3L0C3S-2M0F3Q-6B1N0W-5N737F). Master Console version 0.11.0 ne peut pas être téléchargé séparément.

Pour plus d'informations sur l'utilisation de Master Console, voir le manuel *IBM Security QRadar Master Console*.

Performances améliorées

- Les consoles XX28 prennent désormais en charge 1 million d'actifs, et jusqu'à 3 millions avec une optimisation. Dans QRadar version 7.2.7 et les versions antérieures, le nombre maximal d'actifs pris en charge pour les consoles était 700 000.
- La haute disponibilité n'affecte plus le nombre d'actifs pris en charge. Dans QRadar version 7.2.7 et les versions antérieures, un déploiement avec la haute disponibilité prenait en charge 50 pour cent d'actifs de moins qu'un déploiement sans la haute disponibilité.
- Les requêtes sur les actifs dans l'interface utilisateur sont jusqu'à 35 fois plus rapides. Les requêtes de l'interface utilisateur de vulnérabilité sont désormais deux fois plus rapides.
- Le traitement des événements et des flux est plus efficace, ce qui améliore la stabilité du système et les fonctionnalités de traitement de rafale d'événements de QRadar.
- L'espace disque requis pour chaque événement est réduit de 5%.

Capture de paquet en temps réel avec QRadar Network Packet Capture

QRadar Network Packet Capture permet la capture en temps réel sur disque, avec un stockage utilisable de 66 To pour les captures de paquet. Les performances ont été améliorées avec 10 gigabits par seconde dans toutes les configurations RAID.

Pour plus d'informations, voir le *guide d'installation d'IBM QRadar Network Packet Capture*.

Analyse en temps réel des données réseau avec QRadar Network Insights

QRadar Incident Forensics introduit QRadar Network Insights, un niveau avancé de détection des menaces intégré à IBM Security QRadar. Le nouvel ID de dispositif 6200 est disponible pour déployer QRadar Network Insights.

Pour plus d'informations, voir le *guide d'installation d'IBM Security QRadar Incident Forensics*.

Chapitre 1. Présentation des déploiements de QRadar

Vous pouvez installer IBM Security QRadar sur un serveur unique pour les petites entreprises ou sur plusieurs serveurs pour les environnements des grandes entreprises.

Pour des performances et une évolutivité maximales, vous devez installer un dispositif d'hôte géré haute disponibilité (HD) pour chaque système nécessitant une protection HD. Pour plus d'informations sur l'installation ou la restauration d'un système HD, voir *IBM Security QRadar High Availability Guide*.

Clés d'activation et clés de licence

Lorsque vous installez des dispositifs IBM Security QRadar, vous devez entrer une clé d'activation. Après l'installation, vous devez appliquer les clés de licence. Pour éviter d'entrer une clé incorrecte lors de la procédure d'installation, il est important de comprendre la différence entre les clés.

Clé d'activation

La clé d'activation est une chaîne alphanumérique à 24 caractères, en 4 parties, qui vous est envoyée par IBM. Toutes les installations des produits QRadar utilisent le même logiciel. Cependant, la clé d'activation spécifie les modules logiciels à appliquer pour chaque type de dispositif. Par exemple, utilisez la clé d'activation IBM Security QRadar QFlow Collector pour installer uniquement les modules QRadar QFlow Collector.

Vous pouvez obtenir la clé d'activation aux emplacements suivants :

- Si vous avez acheté un dispositif sur lequel le logiciel QRadar est préinstallé, la clé d'activation figure dans un document sur le CD associé.
- Si vous avez acheté le logiciel QRadar ou le téléchargement du dispositif virtuel, une liste de clés d'activation figure dans le document *Mise en route*. Le document *Mise en route* est joint au courrier électronique de confirmation.

Clé de licence

Votre système inclut une clé de licence temporaire, qui vous permet d'accéder au logiciel QRadar pendant cinq semaines. Une fois que vous avez installé le logiciel et avant l'expiration de la clé de licence par défaut, vous devez ajouter les licences achetées.

Le tableau ci-dessous décrit les restrictions pour la clé de licence par défaut :

Tableau 1. Restrictions de clé de licence par défaut pour les installations de QRadar SIEM

Utilisation	Limite
Limite de source de journal active	750
Seuil d'événements par seconde	5000
Flux par intervalle	200 000
Limite du nombre d'utilisateurs	10
Limite du nombre d'objets réseau	300

Tableau 2. Restrictions de clé de licence par défaut pour les installations de QRadar Log Manager

Utilisation	Limite
Limite de source de journal active	750
Seuil d'événements par seconde	5000
Limite du nombre d'utilisateurs	10
Limite du nombre d'objets réseau	300

Lorsque vous achetez un produit QRadar, IBM vous envoie un courrier électronique contenant votre clé de licence permanente. Ces clés de licence étendent les fonctions de votre type de dispositif et définissent les paramètres e votre système d'exploitation. Vous devez appliquer vos clés de licence avant l'expiration de votre licence par défaut.

Tâches associées:

Chapitre 3, «Installation de QRadar Console ou d'un hôte géré», à la page 17
Installez le composant IBM Security QRadar Console ou un hôte géré sur le dispositif QRadar ou sur votre propre dispositif.

«Installation de RHEL sur votre propre dispositif», à la page 23
Vous pouvez installer le système d'exploitation Red Hat Enterprise Linux sur votre propre dispositif pour l'utiliser avec IBM Security QRadar.

«Installation du logiciel QRadar sur un ordinateur virtuel», à la page 34
Une fois que vous avez créé votre ordinateur virtuel, vous devez y installer le logiciel IBM Security QRadar.

Integrated Management Module

Utilisez Integrated Management Module, qui se trouve sur le panneau arrière de chaque type de dispositif pour la gestion à distance du matériel et des systèmes d'exploitation, indépendamment du statut du serveur géré.

Vous pouvez configurer Integrated Management Module de manière à partager un port Ethernet avec l'interface de gestion des produits IBM Security QRadar. Cependant, pour réduire le risque de perdre la connexion lors du redémarrage du dispositif, configurez Integrated Management Module en mode dédié.

Pour configurer Integrated Management Module, vous devez accéder aux paramètres du BIOS système en appuyant sur la touche F1 lorsque l'écran d'accueil IBM s'affiche. Pour plus d'informations sur la configuration de Integrated Management Module, consultez le manuel *Integrated Management Module - Guide d'utilisation* sur le CD qui accompagne votre dispositif.

Concepts associés:

«Accessoires et logiciels de bureau requis pour les installations de QRadar», à la page 6
Avant d'installer des produits IBM Security QRadar, assurez-vous que vous avez accès aux accessoires et aux logiciels de bureau requis.

Composants QRadar

IBM Security QRadar consolide les données d'événement de sources de journal utilisées par des dispositifs et des applications sur votre réseau.

Important : Les logiciels de tous les dispositifs IBM Security QRadar d'un déploiement doivent être à la même version et au même niveau de correctif. Les déploiements qui utilisent des versions de logiciel différentes ne sont pas prises en charge.

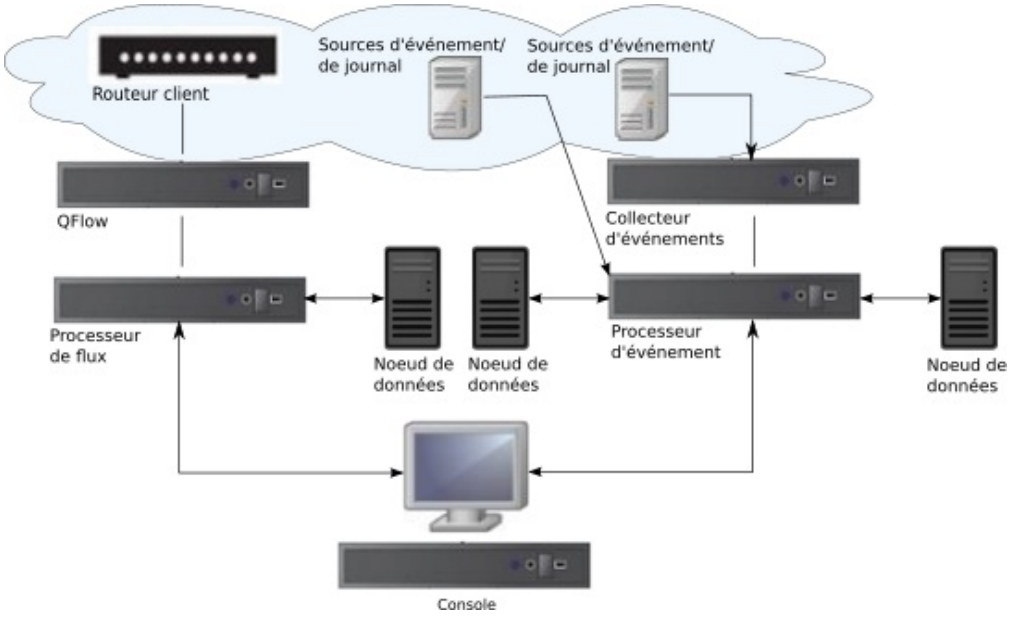

Figure 1. Exemple de déploiement QRadar

Les déploiements QRadar peuvent inclure les composants suivants :

QRadar QFlow Collector
Collecte de façon passive les flux de trafic de votre réseau par le biais de ports SPAN ou d'alertes réseau. IBM Security QRadar QFlow Collector prend également en charge la collecte des sources de données basée sur les flux externes, comme NetFlow.

Vous pouvez installer une instance de QRadar QFlow Collector sur votre propre matériel ou utiliser l'un des dispositifs QRadar QFlow Collector.

Restriction : Le composant est disponible uniquement pour les déploiements QRadar SIEM.

QRadar Console
Fournit l'interface utilisateur du produit QRadar. L'interface fournit des vues d'événements et de flux en temps réel, des rapports, des infractions, des informations sur les actifs et des fonctions d'administration.

Dans les déploiements QRadar distribués, utilisez QRadar Console pour gérer les hôtes incluant d'autres composants.

Magistrat
Un service s'exécutant dans QRadar Console, le Magistrat fournit les composants de traitement central. Vous pouvez ajouter un composant Magistrat pour chaque déploiement. Le Magistrat fournit les vues, les rapports, les alertes et l'analyse du trafic réseau et des événements de sécurité.

Le composant Magistrat traite les événements en les comparant aux règles personnalisées. Si un événement correspond à une règle, le composant Magistrat génère la réponse configurée dans la règle personnalisée.

Par exemple, la règle personnalisée peut indiquer que lorsqu'un événement correspond à la règle, une infraction est créée. S'il n'y a pas de correspondance avec une règle personnalisée, le composant Magistrat utilise les règles par défaut pour traiter l'événement. Une infraction est une alerte traitée en utilisant plusieurs entrées, événements individuels et événements combinés au comportement et aux vulnérabilités analysés. Le composant Magistrat hiérarchise les infractions et affecte une valeur de magnitude basée sur différents facteurs, dont le nombre d'événements, la gravité, la pertinence et la crédibilité.

Collecteur d'événements QRadar

Regroupe les événements des sources de journal locales et distantes. Normalise les événements des sources de journal brutes. Au cours de ce processus, le composant Magistrat, sur QRadar Console, examine l'événement de la source de journal et le mappe à un composant QID (QRadar Identifier). Ensuite, le collecteur d'événements regroupe les événements identiques afin de conserver l'utilisation du système et envoie les informations au processeur d'événement

- Utilisez QRadar Event Collector 1501 dans les emplacements distants avec des liaisons WAN lentes. Les dispositifs du collecteur d'événements n'enregistrent pas les événements en local. En revanche, ces dispositifs collectent et analysent les événements avant de les envoyer à un dispositif du processeur d'événement à des fins de stockage.
- collecteur d'événements peut utiliser des limiteurs de bande passante et des planifications pour l'envoi des événements au processeur d'événement afin d'éviter les limitations de réseau étendu.
- collecteur d'événements est affectée à une licence EPS qui correspond au processeur d'événement auquel il est connecté.

Processeur d'événement QRadar

Traite les événements collectés à partir d'un ou de plusieurs composants collecteur d'événements. Le processeur d'événement corrèle les informations des produits QRadar et distribue les informations à la zone appropriée en fonction du type d'événement. Le processeur d'événement peut également collecter des événements si votre déploiement ne comporte pas de collecteur d'événements.

Le processeur d'événement inclut également les informations regroupées par les produits QRadar pour indiquer les changements de comportement ou les violations des règles pour l'événement. Une fois l'opération terminée, le processeur d'événement envoie les événements au composant Magistrat.

Dans quels cas ajouter des processeurs d'événement

- Si votre débit d'événements dépasse le débit d'un système QRadar 3105 (All-in-One), 5000 EPS, vous devez ajouter QRadar Event Processor 1605 ou QRadar Event Processor 1628.
- Si vous collectez et stockez des événements dans un autre pays ou état, vous devrez peut-être ajouter des processeurs d'événement pour respecter les réglementations locales relatives à la collecte de données.

Noeud de données

Les noeuds de données permettent aux déploiements QRadar nouveaux et existants d'ajouter de la capacité de stockage et de traitement à la demande lorsque cela est nécessaire. Les noeuds de données accroissent la vitesse de recherche dans votre déploiement et vous permettent de conserver davantage de données non compressées.

Pour plus d'informations sur chaque composant, consultez le manuel *Administration Guide*.

Taille du dispositif QRadar

Le tableau ci-dessous contient des indications concernant l'utilisation de dispositifs QRadar spécifiques dans votre déploiement.

Tableau 3. Présentation des dispositifs QRadar

Dispositif	Description
QRadar 2100	Solution qui ne peut pas être étendue pour les déploiements avec 10 à 200 employés.
QRadar 3105 (All-in-One)	Présente une capacité accrue par rapport au système QRadar 2100, et permet d'ajouter des processeurs d'événement et des processeurs de flux.
QRadar 3105 (Console)	Si votre déploiement traite plus de 5000 événements par seconde (EPS), vous devez utiliser un système QRadar 3105 (Console) avec des processeurs d'événement distribués. Le système QRadar 3105 (Console) utilise le traitement d'événement et le stockage externes afin de libérer des ressources pour la mise à disposition de rapports, de résultats de recherche et des actions d'interface utilisateur plus rapides.
QRadar 3128 (All-in-One)	Présente une capacité accrue par rapport au système QRadar 3105 (All-in-One).
QRadar 3128 (Console)	Présente une capacité accrue par rapport au système QRadar 3105 (Console).
Collecteurs et processeurs xx05	12 processeurs 64 Go de mémoire RAM 6,2 To d'espace de stockage utilisable
Collecteurs et processeurs xx28	28 processeurs 128 Go de mémoire RAM 40 To d'espace de stockage utilisable Couplage de collecteurs et processeurs xx28 avec le système QRadar 3128 (Console) pour accroître les performances.

Dans quels cas ajouter des processeurs de flux

- Lorsque votre débit de collecte de NetFlow dépasse l'évaluation de flux pour votre dispositif 31xx, vous devez passer à un processeur de flux dédié.

- Si vous ajoutez des collecteurs QRadar QFlow à votre déploiement, vous devez ajouter des processeurs de flux pour stocker et traiter les données QFlow si vous dépassez la capacité de traitement de votre console.
- Si vous collectez et stockez des flux dans un autre pays ou état, vous devrez peut-être ajouter des processeurs de flux pour respecter les réglementations locales relatives à la collecte de données.

Concepts associés:

Chapitre 11, «Traitement des incidents», à la page 61
Le traitement des incidents est une approche systématique pour résoudre un problème. L'objectif du traitement des incidents est de déterminer pourquoi quelque chose ne fonctionne pas de la façon escomptée et comment résoudre le problème.

Chapitre 9, «Présentation des noeuds de données», à la page 53
Utilisation des noeuds de données dans votre déploiement IBM Security QRadar.

Accessoires et logiciels de bureau requis pour les installations de QRadar

Avant d'installer des produits IBM Security QRadar, assurez-vous que vous avez accès aux accessoires et aux logiciels de bureau requis.

Accessoires

Assurez-vous que vous disposez des composants matériels suivants :

- Ecran et clavier ou console série
- Alimentation de secours pour tous les systèmes de stockage des données, comme QRadar Console, les composants Event Processor ou les composants QRadar QFlow Collector
- Câble de modem null si vous souhaitez connecter le système à une console série

Important : Les produits QRadar prennent en charge les mises en oeuvre matérielles RAID (Redundant Array of Independent Disks), mais ne prennent pas en charge les installations logicielles RAID.

Configuration logicielle de bureau requise

Vérifiez que Java™ Runtime Environment (JRE) version 1.7 ou IBM 64-bit Runtime Environment for Java V7.0 est installé sur tous les systèmes de bureau que vous utilisez pour accéder à l'interface utilisateur du produit de QRadar.

Tâches associées:

Chapitre 3, «Installation de QRadar Console ou d'un hôte géré», à la page 17
Installez le composant IBM Security QRadar Console ou un hôte géré sur le dispositif QRadar ou sur votre propre dispositif.

«Installation de RHEL sur votre propre dispositif», à la page 23
Vous pouvez installer le système d'exploitation Red Hat Enterprise Linux sur votre propre dispositif pour l'utiliser avec IBM Security QRadar.

«Installation du logiciel QRadar sur un ordinateur virtuel», à la page 34
Une fois que vous avez créé votre ordinateur virtuel, vous devez y installer le logiciel IBM Security QRadar.

Mise à jour du microprogramme

Mettez à jour le microprogramme sur les dispositifs IBM Security QRadar afin de pouvoir profiter des avantages des mises à jour et des fonctions supplémentaires pour les composants matériels internes du dispositif QRadar.

Pour plus d'informations sur la mise à jour du microprogramme, voir Firmware update for QRadar (http://www-01.ibm.com/support/docview.wss?uid=swg27047121).

Navigateurs Web pris en charge

Pour que les fonctions des produits IBM Security QRadar fonctionnent correctement, vous devez utiliser un navigateur Web pris en charge.

Lorsque vous accédez au système QRadar, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Les noms d'utilisateur et mot de passe doivent être configurés à l'avance par l'administrateur.

Le tableau ci-après répertorie les versions de navigateurs web pris en charge.

Tableau 4. Navigateurs Web pris en charge par les produits QRadar

Navigateur Web	**Versions prises en charge**
Mozilla Firefox	45.2 Extended Support Release
Microsoft Internet Explorer 64 bits avec le mode Microsoft Edge activé.	11.0
Google Chrome	Latest

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** et sélectionnez l'option **Standards Internet Explorer** correspondant à votre version d'Internet Explorer.

Concepts associés:

«Accessoires et logiciels de bureau requis pour les installations de QRadar», à la page 6
Avant d'installer des produits IBM Security QRadar, assurez-vous que vous avez accès aux accessoires et aux logiciels de bureau requis.

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
- Système Linux sur lequel Red Hat Enterprise Linux v6.8
- 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 dispositif QRadar.
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 de QRadar 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 système Linux de bureau ou portable avec Red Hat v6.8 pour créer une clé USB amorçable, utilisable pour installer le logiciel 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 v6.8
  - 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 Linux.
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 au système Linux en tant que superutilisateur (root).
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 dépend des minuscules/majuscules.
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.

Logiciels tiers sur les dispositifs QRadar

IBM Security QRadar est un dispositif de sécurité basé sur Linux, et conçu pour résister aux attaques. QRadar n'est pas destiné à faire office de serveur multi-utilisateurs et polyvalent. Il est spécialement conçu et développé pour la prise en charge des fonctions prévues. Le système d'exploitation et les services sont prévus pour un fonctionnement sécurisé. QRadar comprend un pare-feu intégré. Il autorise un accès administrateur uniquement via une connexion sécurisée qui exige un accès chiffré et authentifié et garantit des mises à niveau et des mises à niveau contrôlées. QRadar ne nécessite ni n'accepte aucun antivirus ou agent anti-logiciel malveillant traditionnel. Il ne prend pas en charge l'installation de modules ou programmes tiers.

Chapitre 2. Bande passante pour les hôtes gérés

Pour pouvoir répliquer les données d'état et de configuration, vérifiez que vous disposez au minimum d'une bande passante de 100 Mbits/s entre la console IBM Security QRadar et tous les hôtes gérés.

Une bande passante plus large est requise si vous devez effectuer des recherches dans les journaux et l'activité réseau et que votre nombre d'événements par seconde (EPS) dépasse 10000 événements. Les performances de votre système et de votre réseau ont une incidence sur la vitesse de recherche des données. Les collecteurs d'événements QRadar, d'après la configuration de stockage et d'acheminement, envoient toutes les données conformément à votre planning. Vous devez allouer une bande passante suffisante compte tenu des données que vous comptez collecter, faute de quoi votre dispositif de stockage et d'acheminement ne pourra pas suivre le rythme programmé.

Vous pouvez atténuer à l'aide des méthodes suivantes les limitations entre centres de données :

En traitant et en envoyant les données à des hôtes sur le centre de données principal.

En concevant votre déploiement pour un traitement et un envoi des données aux hôtes du centre de données principal, sur lequel réside la console, lors de la collecte de données. De la sorte, toutes les demandes de recherche de l'utilisateur recherchent les données sur le centre de données local au lieu d'attendre leur réacheminement depuis des sites distants. Vous pouvez déployer un collecteur d'événements de stockage et de réacheminement, tel qu'un dispositif QRadar 15XX physique ou virtuel, sur les emplacements distants pour contrôler les pics de données à travers le réseau. La bande de données est utilisée sur les emplacements distants et recherche des données se produisant au centre de données principal, et non pas à un emplacement distant.

N'effectuez pas de recherches de longue durée avec des connexions sur une bande de données étroite

Prenez soin que les utilisateurs n'effectuent pas de recherches de longue durée sur des liens avec une bande de données limitée. Les recherches utilisant des filtres précis limitent la quantité de données extraite depuis l'emplacement distant, tout comme la bande passante nécessaire pour acheminer les données de résultat.

Pour plus d'informations sur le déploiement d'hôtes gérés et de composants après l'installation, reportez-vous au manuel *IBM Security QRadar Administration Guide*.

Chapitre 3. Installation de QRadar Console ou d'un hôte géré

Installez le composant IBM Security QRadar Console ou un hôte géré sur le dispositif QRadar ou sur votre propre dispositif.

Les logiciels de tous les dispositifs QRadar d'un déploiement doivent être à la même version et au même niveau de correctif. Les déploiements qui utilisent différentes versions de logiciel ne sont pas pris en charge.

Avant de commencer

Assurez-vous que les conditions requises ci-dessous sont remplies :

- La configuration matérielle requise est installée.
- Un clavier et un écran sont connectés au moyen d'une connexion VGA.
- La clé d'activation est disponible.
- Si vous voulez configurer des interfaces réseau garanties, voir Configuring network interfaces (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/t_qradar_adm_config_nic_bonding.html).

Procédure

1. Entrez `setup` pour continuer et connectez-vous en tant que superutilisateur.
2. Acceptez le contrat de licence de programme.

   Conseil : Appuyez sur la barre d'espacement pour avancer dans le document.
3. Lorsque vous êtes invité à entrer la clé d'activation, entrez la chaîne alphanumérique à 24 caractères, en 4 parties, qu'IBM vous a envoyée.

   La lettre I et le nombre 1 (un) sont traités de la même façon. La lettre O et le nombre 0 (zéro) sont eux aussi traités de la même façon.
4. Pour le type de configuration, sélectionnez **Normal**, modèle Enterprise, et paramétrez la durée.
5. Sélectionnez la version de protocole IP :
   - Sélectionnez **Oui** pour configurer automatiquement QRadar pour IPv6.
   - Sélectionnez **Non** pour configurer une adresse IP manuellement QRadar pour IPv4 ou IPv6.
6. Sélectionnez l'interface garantie configurée si nécessaire.
7. Sélectionnez l'interface de gestion.
8. Dans l'assistant, entrez un nom de domaine complet dans la zone **Nom d'hôte**.
9. Dans la zone **Adresse IP**, entrez une adresse IP statique ou utilisez l'adresse IP affectée.

   Important : Si vous configurez cet hôte en tant qu'hôte principal pour un cluster à haute disponibilité, et si vous avez sélectionné **Oui** pour la configuration automatique, vous devez enregistrer l'adresse IP générée automatiquement. L'adresse IP générée est entrée lors de la configuration de la haute disponibilité.

   Pour plus d'informations, consultez le manuel *IBM Security QRadar High Availability Guide*.

10. Si vous ne disposez pas d'un serveur de messagerie, entrez `localhost` dans la zone **Nom du serveur de messagerie**.
11. Dans la zone **Mot de passe root**, créez un mot de passe répondant aux critères suivants :
    - Il doit contenir au moins 5 caractères.
    - Il ne doit pas contenir d'espaces.
    - Il peut comporter les caractères spéciaux suivants : @, #, ^ et *.
12. Cliquez sur **Terminer**.
13. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.

    La procédure d'installation peut prendre plusieurs minutes.
14. Appliquez votre clé de licence.
    a. Connectez-vous à QRadar :

       `https://`*`Adresse_IP_QRadar`*

       Le nom d'utilisateur par défaut est `admin`. Le mot de passe est celui du compte de l'utilisateur root.
    b. Cliquez sur **Login To QRadar**.
    c. Cliquez sur l'onglet **Admin**.
    d. Dans le volet de navigation, cliquez sur **Configuration système**.
    e. Cliquez sur l'icône **Gestion du système et de la licence**.
    f. Dans la zone de liste **Afficher**, sélectionnez **Licences**, puis téléchargez votre clé de licence.
    g. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.
    h. Dans la liste de systèmes, sélectionnez un système et cliquez sur **Allouer un système à la licence**.
15. Si vous voulez ajouter des hôtes géré, consultez le manuel *IBM Security QRadar SIEM Administration Guide*.

Que faire ensuite

Accédez à l'adresse (https://apps.xforce.ibmcloud.com/) pour recevoir par téléchargement les *applications de sécurité* adaptées à votre installation. Pour plus d'informations, consultez le chapitre relatif à la *gestion de contenu* dans le manuel *IBM Security QRadar SIEM Administration Guide*.

Chapitre 4. Installations du logiciel QRadar sur votre propre dispositif

Pour garantir la réussite de l'installation d'IBM Security QRadar sur votre propre dispositif, vous devez installer le système d'exploitation Red Hat Enterprise Linux (RHEL).

RHEL est inclus dans l'image ISO du logiciel QRadar et est installé au cours du processus d'installation du logiciel QRadar.

Remarque : L'utilisation de RHEL requiert l'autorisation d'accès au noeud de logiciel QRadar. Pour acquérir cette autorisation, prenez contact avec votre ingénieur commercial QRadar.

Assurez-vous que la configuration système requise pour les déploiements de QRadar est respectée.

Important : n'installez aucun logiciel autre que QRadar et Red Hat Enterprise Linux sur votre dispositif.

Si vous installez le logiciel QRadar sur votre propre matériel, vous devez, pour QRadar version 7.2.8 et les versions ultérieures, acheter la licence RHEL, sous la forme du noeud de logiciel QRadar, et utiliser la copie de REHL livrée avec l'image ISO du logiciel QRadar.

Dans le cadre de l'installation du logiciel QRadar, il n'est pas nécessaire de configurer des partitions ni d'effectuer d'autres tâches de préparation de RHEL. Procédez à l'Chapitre 3, «Installation de QRadar Console ou d'un hôte géré», à la page 17.

Important : tenez compte des mises en garde suivantes :

- Veuillez ne pas installer de modules RPM non approuvés par IBM. Des installations RPM non approuvées peuvent causer aussi bien des erreurs de dépendance lorsque vous mettez à niveau QRadar que des problèmes de performance lors du déploiement.
- Veuillez ne pas utiliser YUM pour mettre à jour votre système d'exploitation ou pour installer des logiciels non approuvés sur des systèmes QRadar.

Configuration requise pour l'installation de QRadar sur votre propre dispositif

Avant d'installer le système d'exploitation Red Hat Enterprise Linux (RHEL) sur votre dispositif, assurez-vous que votre système respecte la configuration système requise.

RHEL est inclus dans l'image ISO du logiciel QRadar et est installé au cours du processus d'installation du logiciel QRadar. L'utilisation de RHEL requiert l'autorisation d'accès au noeud de logiciel QRadar. Pour acquérir cette autorisation, prenez contact avec votre ingénieur commercial QRadar.

Le tableau ci-dessous décrit la configuration système requise :

Tableau 5. Configuration système requise pour les installations RHEL sur votre propre dispositif

Conditions requises	Description
Version de logiciel prise en charge	Version v6.8
Version de bits	64 bits
Disques KickStart	Pas pris en charge
Module NTP (Network Time Protocol)	Facultatif Si vous voulez utiliser le module NTP comme serveur de temps, veillez à l'installer.
Mémoire (vive) pour les systèmes de console	32 Go minimum **Important :** Vous devez mettre la mémoire de votre système à niveau avant d'installer QRadar.
Mémoire (vive) pour processeur d'événement	24 Go
Mémoire (vive) pour QRadar QFlow Collector	16 Go
Espace disque disponible pour les systèmes de console	256 Go minimum **Important :** pour des performances optimales, assurez-vous qu'un espace égal à 2 ou 3 fois l'espace disque minimal est disponible.
Lecteur principal QRadar QFlow Collector	70 Go minimum
Configuration de pare-feu	Compatible WWW (http, https) Compatible SSH **Important :** avant de configurer le pare-feu, désactivez l'option SELinux. L'installation de QRadar inclut un modèle de pare-feu par défaut que vous pouvez mettre à jour dans la fenêtre Configuration du système.

Remarque : Les installations EFI ne sont pas prises en charge.

Configuration minimale requise des dispositifs pour les installations virtuelles et logicielles

Pour installer QRadar dans une configuration virtuelle ou logicielle, vous devez disposer d'une configuration minimale.

Le tableau suivant présente la configuration minimale recommandée pour installer QRadar dans une configuration virtuelle ou logicielle uniquement.

Remarque : La quantité de stockage minimale peut varier en fonction d'un certain nombre de facteurs, comme la taille des événements, le nombre d'événements par seconde (EPS) et les règles de conservation.

Tableau 6. Configuration minimale requise pour les dispositifs lors d'une installation virtuelle ou logicielle.

Classification système	Informations sur le dispositif	IOPS	Vitesse de transfert des données (Mo/s)
Performances minimales	Prise en charge de la gestion de licence XX05	800	500
Performances moyennes	Prise en charge de la gestion de licence XX28	1200	1000
Hautes performances	Prise en charge de la gestion de licence XX48	10000	2000
Small All-in-One ou 1600	Moins de 500 EPS	300	300
Collecteurs d'événements/flux	Evénements et flux	300	300

Préparation des installations du logiciel QRadar pour les systèmes de fichiers XFS

Dans le cadre de la configuration haute disponibilité (HD), le programme d'installation de QRadar nécessite un espace disponible minimal sur le système de fichiers de stockage, `/store/`, pour les procédures de réplication. L'espace doit être alloué à l'avance, car la taille des systèmes de fichiers XFS ne peut pas être réduite une fois qu'ils ont été formatés.

Pour préparer la partition XFS, vous devez procéder comme suit :

1. Utilisez la commande **`mkdir`** pour créer les répertoires suivants :
   - `/media/cdrom`
   - `/media/redhat`
2. Montez l'image ISO du logiciel QRadar en entrant la commande suivante :

   `mount -o loop <chemin d'accès à l'image ISO de QRadar> /media/cdrom`
3. Montez le logiciel RedHat Enterprise Linux v6.8 en exécutant la commande suivante :

   `mount -o loop <path_to_RedHat_6.8_64bit_dvd_iso_1> /media/redhat`
4. Si votre système est désigné comme hôte principal dans une paire HD, exécutez le script suivant :

   `/media/cdrom/post/prepare_ha.sh`

   Important : L'exécution de cette commande sur un serveur autonome existant reformate la partition de stockage et entraîne une perte de données.
5. Pour commencer l'installation, entrez la commande suivante :

   `/media/cdrom/setup`

Propriétés de la partition du système d'exploitation Linux pour les installations QRadar sur votre propre dispositif

Si vous utilisez votre propre dispositif, vous pouvez supprimer et recréer des partitions sur votre système d'exploitation Red Hat Enterprise Linux au lieu de modifier les partitions par défaut.

Utilisez les valeurs dans le tableau suivant comme guide lorsque vous recréez le partitionnement sur votre système d'exploitation Red Hat Enterprise Linux.

Restriction : Le redimensionnement des volumes logiques avec un gestionnaire de volumes logiques n'est pas pris en charge.

Tableau 7. Guide de partitionnement pour RHEL

Partition	Description	Point de montage	Type de système de fichiers	Taille	Le principal doit être forcé.	SDA/SDB
/boot	Fichiers d'amorçage système	/boot	EXT4	200 MB	Oui	SDA
permutation	Utilisé comme mémoire lorsque la mémoire vive est saturée.	vide	permutation	Systèmes dotés de 4 à 8 Go de mémoire vive. La taille de la partition de permutation doit correspondre à la quantité de mémoire vive. Systèmes dotés de 8 à 24 Go de mémoire vive. Configurez la taille de la partition de permutation pour qu'elle corresponde à 75% de la mémoire vive, avec une valeur minimale de 8 Go et une valeur maximale de 24 Go.	Non	SDA
/	Zone d'installation pour QRadar, le système d'exploitation et les fichiers associés.	/	EXT4	20 000 Mo	Non	SDA
/store/tmp	Zone de stockage pour les fichiers temporaires QRadar	/store/tmp	EXT4	20 000 Mo	Non	SDA
/var/log	Zone de stockage pour les fichiers journaux QRadar et système	/var/log	EXT4	20 000 Mo	Non	SDA

Tableau 7. Guide de partitionnement pour RHEL (suite)

Partition	Description	Point de montage	Type de système de fichiers	Taille	Le principal doit être forcé.	SDA/SDB
/store	Zone de stockage pour les données et les fichiers de configuration de QRadar	/store	XFS	[1]Sur les dispositifs de la console : environ 80 % de l'espace de stockage disponible. Sur les hôtes gérés autres que des collecteurs QFlow et des collecteurs d'événements de stockage et de transfert : environ 90 % de l'espace de stockage disponible.	Non	SDA S'il y a deux disques, SDB
/store/transient	Zone de stockage pour le curseur de base de données ariel	/store/transient	XFS sur les consoles EXT4 sur les hôtes gérés	[1]Sur les dispositifs de la console : 20 % de l'espace de stockage disponible. Sur les hôtes gérés autres que des collecteurs QFlow et des collecteurs d'événements de stockage et de transfert : 10 % de l'espace de stockage disponible.	Non	SDA S'il y a deux disques, SDB
[1]Les fichiers /store et /store/transient occupent la totalité de l'espace disque restant après la création des cinq premières partitions.						

Restrictions

Les mises à niveau logicielles futures peuvent échouer si vous reformatez l'une des partitions ou sous-partitions suivantes :

- /store
- /store/tmp
- /store/ariel
- /store/transient

Installation de RHEL sur votre propre dispositif

Vous pouvez installer le système d'exploitation Red Hat Enterprise Linux sur votre propre dispositif pour l'utiliser avec IBM Security QRadar.

Pourquoi et quand exécuter cette tâche

RHEL est inclus dans l'image ISO du logiciel QRadar et est installé au cours du processus d'installation du logiciel QRadar. L'utilisation de RHEL requiert

l'autorisation d'accès au noeud de logiciel QRadar. Pour acquérir cette autorisation, prenez contact avec votre ingénieur commercial QRadar.

Si vous devez installer RHEL séparément, suivez les instructions ci-après. Sinon, passez à la rubrique Chapitre 4, «Installations du logiciel QRadar sur votre propre dispositif», à la page 19.

Procédure

1. Copiez l'image ISO du DVD du système d'exploitation Red Hat Enterprise Linux v6.8 sur l'un des périphériques de stockage portables suivants :
   - DVD
   - Lecteur USB amorçable
2. Connectez le périphérique de stockage portable au dispositif et redémarrez le dispositif.
3. Depuis le menu de démarrage, effectuez l'une des opérations suivantes :
   - Sélectionnez le lecteur USB ou DVD comme option d'amorçage.
   - Pour effectuer l'installation sur un système prenant en charge l'interface de microprogramme extensible, vous devez démarrer le système en mode `propriétaire`.
4. Lorsque vous y êtes invité, connectez-vous au système comme utilisateur root.
5. Pour empêcher un problème avec le nommage des adresses d'interface Ethernet, dans la page d'accueil, appuyez sur la touche de tabulation et à la fin de la ligne `Vmlinuz initrd=initrd.image`, ajoutez `biosdevname=0`.
6. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation :
   a. Sélectionnez l'option **Périphériques de stockage standard**.
   b. Lorsque vous configurez le nom d'hôte, la propriété **Nom d'hôte** peut inclure des lettres, des nombres et des tirets.
   c. Lorsque vous configurez le réseau, dans la fenêtre Connexions réseau, sélectionnez **Système eth0**, puis cliquez sur **Modifier** et sélectionnez **Se connecter automatiquement**.
   d. Sous l'onglet **Paramètres IPv4**, dans la liste **Méthode**, sélectionnez **Manuelle**.
   e. Dans la zone **Serveurs DNS**, entrez une liste de valeurs séparées par des virgules.
   f. Sélectionnez l'option **Créer une présentation personnalisée**.
   g. Configurez `EXT4` comme type de système de fichiers pour les partitions `/`, `/boot`, `/store/tmp` et `/var/log`.

      Pour plus d'informations sur les types de système de fichiers basés sur les types de dispositifs, voir «Propriétés de la partition du système d'exploitation Linux pour les installations QRadar sur votre propre dispositif», à la page 21.
   h. Reformatez la partition de permutation avec le type de système de fichiers permutation.
   i. Sélectionnez **Serveur standard**.
7. Une fois l'installation terminée, cliquez sur **Redémarrer**.

Que faire ensuite

Après l'installation, si un nom autre que `eth0`, `eth1`, `eth2` et `eth3` est attribué à vos interfaces, vous devez renommer les interfaces réseau.

Référence associée:

«Propriétés de la partition du système d'exploitation Linux pour les installations QRadar sur votre propre dispositif», à la page 21
Si vous utilisez votre propre dispositif, vous pouvez supprimer et recréer des partitions sur votre système d'exploitation Red Hat Enterprise Linux au lieu de modifier les partitions par défaut.

Chapitre 5. Installations de dispositif virtuel pour QRadar SIEM et QRadar Log Manager

Vous pouvez installer IBM Security QRadar SIEM et IBM QRadar Log Manager sur un dispositif virtuel. Assurez-vous que vous utilisez un dispositif virtuel pris en charge respectant la configuration système requise minimale.

Restriction : Le redimensionnement des volumes logiques en utilisant un gestionnaire de volumes locaux et les installations EFI ne sont pas pris en charge.

Red Hat Enterprise Linux (RHEL) est inclus dans l'image ISO du logiciel QRadar et est installé au cours du processus d'installation du logiciel QRadar. L'utilisation de RHEL requiert l'autorisation d'accès au noeud de logiciel QRadar. Pour acquérir cette autorisation, prenez contact avec votre ingénieur commercial QRadar.

Pour installer un dispositif virtuel, exécutez les tâches suivantes dans l'ordre indiqué :

- Créez un ordinateur virtuel.
- Installez le logiciel QRadar sur l'ordinateur virtuel.
- Ajoutez votre dispositif virtuel au déploiement.

Important : N'installez aucun logiciel autre que QRadar et Red Hat Enterprise Linux sur la machine virtuelle.

Présentation des dispositifs virtuels pris en charge

Un dispositif virtuel est un système IBM Security QRadar, qui comprend le logiciel QRadar installé sur un ordinateur virtuel VMWare ESXi .

Un dispositif virtuel confère à votre infrastructure de réseau virtuel la même visibilité et le même fonctionnement que les dispositifs QRadar dans votre environnement physique.

Une fois que vous avez installé vos dispositifs virtuels, utilisez l'éditeur de déploiement pour ajouter vos dispositifs virtuels à votre déploiement. Pour plus d'informations sur la connexion des dispositifs, consultez le manuel *Administration Guide*.

Les dispositifs virtuels disponibles sont les suivants :

- QRadar SIEM All-in-One Virtual 3199
- QRadar SIEM Event and Flow Processor Virtual 1899
- QRadar SIEM Flow Processor Virtual 1799
- QRadar SIEM Event Processor Virtual 1699
- QRadar Data Node Virtual 1400
- QRadar VFlow Collector 1299

QRadar SIEM All-in-One Virtual 3199

Ce dispositif virtuel est un système QRadar SIEM, qui analyse le comportement du réseau et identifie les menaces pour la sécurité du réseau. Le dispositif virtuel QRadar SIEM All-in-One Virtual 3199 inclut un collecteur d'événements intégré et un stockage interne pour les événements.

Le dispositif virtuel QRadar SIEM All-in-One Virtual 3199 prend en charge les éléments suivants :

- Jusqu'à 1000 objets réseau
- 50 000 flux par intervalle, en fonction de votre licence
- 5000 événements par seconde, en fonction de votre licence
- 750 fils d'événements (vous pouvez ajouter d'autres dispositifs à votre licence)
- Sources de données de flux externes pour les fichiers NetFlow, sFlow, J-Flow, Packeteer et Flowlog
- Contrôle de l'activité réseau QRadar QFlow Collector et Layer 7

Pour étendre la capacité de QRadar SIEM All-in-One Virtual 3199 au-delà des options de mise à niveau sous licence, vous pouvez ajouter un ou plusieurs dispositifs virtuels QRadar SIEM Event Processor Virtual 1699 ou QRadar SIEM Flow Processor Virtual 1799 :

QRadar SIEM Event and Flow Processor Virtual 1899

Ce dispositif virtuel est déployé avec un composant QRadar Console. Ce dispositif virtuel est utilisé pour augmenter le stockage et inclut un processeur d'événement et un processeur de flux combinés et un stockage interne pour des événements et des flux.

Le dispositif QRadar SIEM Event and Flow Processor Virtual 1899 prend en charge les éléments suivants :

- 200 000 flux par intervalle, en fonction des types de trafic
- 5000 événements par seconde, en fonction de votre licence
- Stockage de flux dédié de 2 To ou plus
- 1000 objets réseau
- Contrôle de l'activité réseau QRadar QFlow Collector et Layer 7

Vous pouvez ajouter des dispositifs QRadar SIEM Event and Flow Processor Virtual 1899 à n'importe quel composant QRadar Console pour augmenter la quantité de stockage et les performances de votre déploiement.

QRadar SIEM Flow Processor Virtual 1799

Ce dispositif virtuel est déployé avec un dispositif série QRadar SIEM 3105 ou QRadar SIEM 3124. Le dispositif virtuel est utilisé pour augmenter le stockage et inclut un processeur d'événement intégré.

Le dispositif QRadar SIEM Flow Processor Virtual 1799 prend en charge les éléments suivants :

- 600 000 flux par intervalle, en fonction des types de trafic
- Stockage de flux dédié de 2 To ou plus
- 1000 objets réseau

- Contrôle de l'activité réseau QRadar QFlow Collector et Layer 7

Vous pouvez ajouter des dispositifs QRadar SIEM Flow Processor Virtual 1799 à un dispositif de série QRadar SIEM 3105 ou QRadar SIEM 3124 pour augmenter le stockage et les performances de votre déploiement.

QRadar SIEM Event Processor Virtual 1699

Ce dispositif virtuel est un processeur d'événement dédié que vous pouvez utiliser pour échelonner votre déploiement QRadar SIEM afin de gérer des taux d'événements par seconde plus élevés. Le dispositif QRadar SIEM Event Processor Virtual 1699 inclut un collecteur d'événements intégré, un processeur d'événement et un stockage interne pour les événements.

Le dispositif QRadar SIEM Event Processor Virtual 1699 prend en charge les éléments suivants :

- Jusqu'à 20 000 événements par seconde
- Stockage d'événements dédié de 2 To ou plus

Le dispositif virtuel QRadar SIEM Event Processor Virtual 1699 est un dispositif processeur d'événement distribué, qui nécessite une connexion à un dispositif série QRadar SIEM 3105 ou QRadar SIEM 3124.

QRadar Data Node Virtual 1400

Ce dispositif virtuel permet de conserver et de stocker les événements et les flux. Le dispositif virtuel étend le stockage de données disponible des processeurs d'événement et des processeurs de flux, et améliore également les performances de recherche.

Remarque : la transmission de données chiffrées entre les noeuds de données et les processeurs d'événement n'est pas prise en charge. Les ports de pare-feu suivants doivent être ouverts pour la communication entre les noeuds de données et le processeur d'événement :

- Port 32006 entre les noeuds de données et le dispositif Processeur d'événement
- Port 32011 entre les noeuds de données et le processeur d'événement de la console

Ajustez la taille de votre Dispositif QRadar Data Node Virtual 1400 en fonction du taux d'événements par seconde et des règles de conservation des données du déploiement.

Les règles de conservation des données sont appliquées à un Dispositif QRadar Data Node Virtual 1400 de la même façon qu'elles sont appliquées à des processeurs d'événement et processeurs de flux autonomes. Les règles de conservation des données sont évaluées noeud par noeud. Les critères, comme l'espace disponible, sont basés sur le Dispositif QRadar Data Node Virtual 1400 et non sur le cluster dans son intégralité.

noeuds de données peut être ajouté aux dispositifs suivants :

- Processeur d'événement (16XX)
- Processeur de flux (17XX)
- Processeur d'événement/de flux (18XX)
- Tout-en-un (2100 et 31XX)

Pour activer toutes les fonctions incluses dans le Dispositif QRadar Data Node Virtual 1400, effectuez l'installation avec la clé d'activation 1400.

QRadar VFlow Collector 1299

Ce dispositif virtuel confère à votre infrastructure de réseau virtuel la même visibilité et le même fonctionnement qu'un dispositif QRadar QFlow Collector dans votre environnement physique. Le dispositif virtuel QRadar QFlow Collector analyse le comportement réseau et fournit la visibilité Layer 7 dans votre infrastructure virtuelle. La visibilité réseau est obtenue par une connexion directe au commutateur virtuel.

Le dispositif virtuel QRadar VFlow Collector 1299 prend en charge un maximum des éléments suivants :

- 10 000 flux par minute
- Trois commutateurs virtuels, avec un commutateur supplémentaire désigné comme interface de gestion.

Le dispositif virtuel QRadar VFlow Collector 1299 ne prend pas en charge NetFlow.

Configuration système requise pour les dispositifs virtuels

Pour vous assurer que IBM Security QRadar fonctionne correctement, vérifiez que le dispositif virtuel que vous utilisez est conforme à la configuration logicielle et matérielle requise minimale.

Avant d'installer votre dispositif virtuel, assurez-vous que la configuration minimale ci-dessous est respectée :

Tableau 8. Configuration requise pour les dispositifs virtuels

Conditions requises	Description
Client VMware	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 Pour plus d'informations sur les clients VMWare, consultez le site web VMware (www.vmware.com)
Taille du disque virtuel sur les dispositifs	Minimum : 256 Go pour installer QRadar

Le tableau ci-dessous décrit la mémoire requise minimale pour les dispositifs virtuels.

Tableau 9. Mémoire requise minimale et facultative pour les dispositifs virtuels QRadar

Dispositif	Mémoire requise minimale	Mémoire requise recommandée
QRadar VFlow Collector 1299	6 Go	6 Go
Dispositif QRadar Data Node Virtual 1400	12 Go	48 Go

Tableau 9. Mémoire requise minimale et facultative pour les dispositifs virtuels QRadar (suite)

Dispositif	Mémoire requise minimale	Mémoire requise recommandée
QRadar Event Collector Virtual 1599	12 Go	16 Go
QRadar SIEM Event Processor Virtual 1699	12 Go	48 Go
QRadar SIEM Flow Processor Virtual 1799	12 Go	48 Go
QRadar SIEM All-in-One Virtual 3199	24 Go	48 Go
QRadar Log Manager Virtual 3190	24 Go	48 Go
QRadar Risk Manager	24 Go	48 Go
Processeur QRadar Vulnerability Manager	32 Go	32 Go
Scanner QRadar Vulnerability Manager	16 Go	16 Go

Tableau 10. Exemple de paramètres de la page **CPU**

Nombre de processeurs	Performances basées sur les dispositifs QRadar
4	Gestionnaire de journaux 3190 : 2500 événements par seconde ou moins. Processeur d'événement du gestionnaire de journaux 1690 ou Processeur d'événement SIEM 1690 : 2500 événements par seconde ou moins. All-in-One 3190 : 25 000 flux par minute ou moins, 500 événements par seconde ou moins. Flow Processor 1790 : 150 000 flux par minute. Console dédiée 3190
8	Gestionnaire de journaux 3190 : 5000 événements par seconde ou moins. Processeur d'événement du gestionnaire de journaux 1690 ou Processeur d'événement SIEM 1690 : 5000 événements par seconde ou moins. All-in-One 3190 : 50 000 flux par minute ou moins, 1000 événements par seconde ou moins. Flow Processor 1790 : 300 000 flux par minute.
12	All-in-One 3190 : 100 000 flux par minute ou moins, 1000 événements par seconde ou moins.
16	Processeur d'événement du gestionnaire de journaux 1690 ou Processeur d'événement SIEM 1690 : 20 000 événements par seconde ou moins. All-in-One 3190 : 200 000 flux par minute ou moins, 5000 événements par seconde ou moins.

Tableau 10. Exemple de paramètres de la page **CPU** *(suite)*

Nombre de processeurs	**Performances basées sur les dispositifs QRadar**
4	Scanner QRadar Vulnerability Manager Utilisez 4 unités centrales pour des performances optimales.
4	Processeur QRadar Vulnerability Manager Utilisez 4 unités centrales pour des performances optimales.
8	QRadar Risk Manager Utilisez 8 unités centrales pour des performances optimales.

Le tableau suivant présente la quantité de stockage minimale recommandée pour installer QRadar en utilisant l'option de configuration virtuelle ou logicielle uniquement.

Remarque : La quantité de stockage minimale peut varier en fonction d'un certain nombre de facteurs, comme la taille des événements, le nombre d'événements par seconde (EPS) et les règles de conservation.

Tableau 11. Configuration minimale requise pour les dispositifs lors d'une installation virtuelle ou logicielle.

Classification système	Informations sur le dispositif	IOPS	Vitesse de transfert des données (Mo/s)
Performances minimales	Prise en charge de la gestion de licence XX05	800	500
Performances moyennes	Prise en charge de la gestion de licence XX28	1200	1000
Hautes performances	Prise en charge de la gestion de licence XX48	10000	2000
Small All-in-One ou 1600	Moins de 500 EPS	300	300
Collecteurs d'événements/flux	Evénements et flux	300	300

Tâches associées:

«Création de votre ordinateur virtuel»
Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESX pour créer un ordinateur virtuel.

Création de votre ordinateur virtuel

Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESX pour créer un ordinateur virtuel.

Procédure

1. Depuis VMware vSphere Client, sélectionnez **Fichier** > **Nouveau** > **Machine virtuelle**.
2. Ajoutez les **Nom et l'emplacement**, et sélectionnez le **Magasin de données** pour la nouvelle machine virtuelle.
3. Pour faciliter votre choix, servez-vous des étapes ci-dessous comme référence :
   a. Dans le volet **Configuration** de l'assistant Créer une nouvelle machine virtuelle, sélectionnez **Personnalisée**.
   b. Dans le volet **Nouvelle machine virtuelle**, sélectionnez **Machine virtuelle de version 7**.
   c. Pour le **système d'exploitation**, sélectionnez **Linux** et **Red Hat Enterprise Linux 6 (64 bits)**.
   d. Sur la page **UC**, configurez le nombre de processeurs virtuels voulus pour la machine virtuelle. Pour plus d'informations sur les paramètres d'UC, voir Configuration système requise pour les dispositifs virtuels.
   e. Dans la zone **Taille de mémoire**, entrez ou sélectionnez la mémoire RAM requise pour votre déploiement. Pour plus d'informations sur les exigences concernant la mémoire, voir Configuration système requise pour les dispositifs virtuels.
   f. Utilisez le tableau ci-dessous pour configurer les connexions réseau.

Tableau 12. Descriptions des paramètres de configuration réseau

Paramètre	Description
Nombre de NIC à connecter	Vous devez ajouter au moins une carte d'interface réseau.

Tableau 12. Descriptions des paramètres de configuration réseau (suite)

Paramètre	Description
Adaptateur	VMXNET3

g. Dans le volet **Contrôleur SCSI**, sélectionnez **VMware Paravirtual**.

h. Dans le volet **Disque**, sélectionnez **Créer un disque virtuel** et utilisez le tableau ci-dessous pour configurer les paramètres du disque virtuel.

Tableau 13. Paramètres de taille de disque virtuel et paramètres de règles de mise à disposition

Propriété	Option
Capacité	256 Go (ou plus) pour l'installation. Votre capacité de stockage dépend du débit d'événements, de leur taille moyenne, et des exigences de conservation.
Mise à disposition des disques	Mise à disposition à la demande
Options avancées	Ne pas configurer

4. Dans la page **Prêt à Terminer**, vérifiez les paramètres et cliquez sur **Terminer**.

Que faire ensuite

Installez les logiciels QRadar sur votre machine virtuelle.

Installation du logiciel QRadar sur un ordinateur virtuel

Une fois que vous avez créé votre ordinateur virtuel, vous devez y installer le logiciel IBM Security QRadar.

Avant de commencer

Assurez-vous que la clé d'activation est disponible.

Procédure

1. Dans le volet de navigation de gauche de votre VMware vSphere Client, sélectionnez votre ordinateur virtuel.
2. Dans le volet de droite, cliquez sur l'onglet **Résumé**.
3. Dans le volet **Commandes**, cliquez sur **Modifier les paramètres**.
4. Dans le volet de gauche de la fenêtre **Propriétés de l'ordinateur virtuel**, cliquez sur **Lecteur de CD/DVD 1**.
5. Dans le panneau **Type d'unité**, sélectionnez **DataStore ISO File**.
6. Dans le volet **Statut du périphérique**, cochez la case **Se connecter au démarrage**.
7. Dans le panneau **Type d'unité**, cliquez sur **Parcourir**.
8. Dans la fenêtre Rechercher dans les magasins de données, recherchez et sélectionnez le fichier ISO du produit QRadar, cliquez sur **Ouvrir**, puis sur **OK**.
9. Après l'installation de l'image ISO du produit QRadar, cliquez avec le bouton droit de la souris sur votre ordinateur virtuelle et cliquez sur **Alimentation** > **Allumer**.

10. Connectez-vous à l'ordinateur virtuel en entrant `root` comme nom d'utilisateur.

    Le nom d'utilisateur dépend des minuscules/majuscules.
11. Assurez-vous que le contrat de licence d'utilisateur final (EULA) est affiché.

    Conseil : Appuyez sur la barre d'espacement pour avancer dans le document.
12. Lorsque vous êtes invité à entrer la clé d'activation, entrez la chaîne alphanumérique à 24 caractères, en 4 parties, qu'IBM vous a envoyée.

    La lettre I et le nombre 1 (un) sont traités de la même façon. La lettre O et le nombre 0 (zéro) sont eux aussi traités de la même façon.
13. Pour le type de configuration, sélectionnez **Normal**, modèle Enterprise, et paramétrez la durée.
14. Sélectionnez la version de protocole IP :
    - Sélectionnez **Oui** pour configurer automatiquement QRadar pour IPv6.
    - Sélectionnez **Non** pour configurer une adresse IP manuellement QRadar pour IPv4 ou IPv6.
15. Sélectionnez l'interface garantie configurée si nécessaire.
16. Sélectionnez l'interface de gestion.
17. Dans l'assistant, entrez un nom de domaine complet dans la zone **Nom d'hôte**.
18. Dans la zone **Adresse IP**, entrez une adresse IP statique ou utilisez l'adresse IP affectée.

    Important : Si vous configurez cet hôte en tant qu'hôte principal pour un cluster à haute disponibilité, et si vous avez sélectionné **Oui** pour la configuration automatique, vous devez enregistrer l'adresse IP générée automatiquement. L'adresse IP générée est entrée lors de la configuration de la haute disponibilité.

    Pour plus d'informations, consultez le manuel *IBM Security QRadar High Availability Guide*.
19. Si vous ne disposez pas d'un serveur de messagerie, entrez `localhost` dans la zone **Nom du serveur de messagerie**.
20. Dans la zone **Mot de passe root**, créez un mot de passe répondant aux critères suivants :
    - Il doit contenir au moins 5 caractères.
    - Il ne doit pas contenir d'espaces.
    - Il peut comporter les caractères spéciaux suivants : @, #, ^ et *.
21. Cliquez sur **Terminer**.
22. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.

    La procédure d'installation peut prendre plusieurs minutes.
23. Appliquez votre clé de licence.
    a. Connectez-vous à QRadar :

       `https://`*`Adresse_IP_QRadar`*

       Le nom d'utilisateur par défaut est `admin`. Le mot de passe est celui du compte de l'utilisateur root.
    b. Cliquez sur **Login To QRadar**.
    c. Cliquez sur l'onglet **Admin**.
    d. Dans le volet de navigation, cliquez sur **Configuration système**.
    e. Cliquez sur l'icône **Gestion du système et de la licence**.

f. Dans la zone de liste **Afficher**, sélectionnez **Licences**, puis téléchargez votre clé de licence.
g. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.
h. Dans la liste de systèmes, sélectionnez un système et cliquez sur **Allouer un système à la licence**.

Que faire ensuite

Accédez à l'adresse (https://apps.xforce.ibmcloud.com/) pour recevoir par téléchargement les *applications de sécurité* adaptées à votre installation. Pour plus d'informations, consultez le chapitre relatif à la *gestion de contenu* dans le manuel *IBM Security QRadar SIEM Administration Guide*.

Tâches associées:

«Création de votre ordinateur virtuel», à la page 33
Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESX pour créer un ordinateur virtuel.

Ajout du dispositif virtuel à votre déploiement

Une fois le logiciel IBM Security QRadar installé, ajoutez le dispositif virtuel à votre déploiement.

Procédure

1. Connectez-vous à QRadar Console.
2. Sous l'onglet **Admin**, cliquez sur l'icône **Editeur de déploiement**.
3. Dans le volet **Composants d'événement** de la page **Affichage des événements**, sélectionnez le composant de dispositif virtuel à ajouter.
4. Dans la première page de l'assistant de la tâche **Ajout d'un nouveau composant**, entrez un nom unique pour le dispositif virtuel.

   Le nom que vous affectez au dispositif virtuel peut comporter 20 caractères et peuvent inclure des traits de soulignement et des tirets.
5. Exécutez les étapes de l'assistant de la tâche.
6. Dans le menu **Editeur de déploiement**, sélectionnez **Fichier** > **Enregistrer lors du transfert**.
7. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les modifications**.
8. Appliquez votre clé de licence.
   a. Connectez-vous à QRadar :

      `https://Adresse_IP_QRadar`

      Le nom d'utilisateur par défaut est `admin`. Le mot de passe est celui du compte de l'utilisateur root.
   b. Cliquez sur **Login To QRadar**.
   c. Cliquez sur l'onglet **Admin**.
   d. Dans le volet de navigation, cliquez sur **Configuration système**.
   e. Cliquez sur l'icône **Gestion du système et de la licence**.
   f. Dans la zone de liste **Afficher**, sélectionnez **Licences**, puis téléchargez votre clé de licence.
   g. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.

h. Dans la liste de systèmes, sélectionnez un système et cliquez sur **Allouer un système à la licence**.

Tâches associées:

«Création de votre ordinateur virtuel», à la page 33
Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESX pour créer un ordinateur virtuel.

Chapitre 6. Installation à partir de la partition de restauration

Lorsque vous installez des produits IBM Security QRadar, le programme d'installation (image ISO) est copié dans la partition de restauration. Dans cette partition, vous pouvez réinstaller les produits QRadar. La configuration par défaut de votre système est rétablie. Vos fichiers de configuration et de données actuels sont remplacés.

Lorsque vous redémarrez le dispositif QRadar, une option de réinstallation du logiciel s'affiche. Si vous ne répondez pas à l'invite dans les 5 secondes, le système continue à démarrer normalement. Vos fichiers de configuration et de données sont conservés. Si vous sélectionnez l'option de réinstallation, un message d'avertissement s'affiche et vous devez confirmer que vous souhaitez effectuer la réinstallation.

Le message d'avertissement indique que vous pouvez conserver les données sur le dispositif. Ces données comprennent les événements et les flux. Sélectionner l'option de conservation sauvegarde les données avant l'installation et restaure les données après l'installation. Si l'option de conservation n'est pas disponible, la partition où les données résident peut ne pas être disponible, et il n'est pas possible de sauvegarder et restaurer les données. L'absence de l'option de conservation peut indiquer une panne du disque dur. Contactez l'assistance clientèle si l'option de conservation n'est pas disponible.

Important : L'option de conservation n'est pas disponible sur les systèmes de haute disponibilité. Voir *IBM Security QRadar High Availability Guide* pour plus d'informations sur la récupération de dispositifs de haute disponibilité.

Les mises à niveau de logiciel de QRadar version 7.2.0 remplacent le fichier ISO existant par le fichier ISO de la nouvelle version.

Ces instructions concernent les nouvelles installations ou les mises à niveau de QRadar version 7.2.0 à partir de nouvelles installations de QRadar version 7.0 sur des dispositifs QRadar version 7.0.

Réinstallation à partir de la partition de restauration

Vous pouvez réinstaller les produits IBM Security QRadar à partir de la partition de restauration.

Avant de commencer

Recherchez votre clé d'activation. La clé d'activation est une chaîne alphanumérique à 24 caractères, en 4 parties, qui vous est envoyée par IBM. Vous pouvez trouver la clé d'activation à l'un des emplacements suivants :

- Elle peut être imprimée sur un autocollant et apposée sur votre dispositif.
- Elle peut être incluse avec le bon de livraison. Tous les dispositifs sont répertoriés avec les clés associées.

Si vous ne disposez pas de votre clé d'activation, accédez au site Web du support IBM (www.ibm.com/support) pour l'obtenir. Vous devez indiquer le numéro de série du dispositif QRadar. Les clés d'activation du logiciel ne nécessitent pas de numéro de série.

Si votre déploiement inclut des solutions de stockage externes, vous devez déconnecter votre espace de stockage externe avant de réinstaller QRadar. Après la réinstallation, vous pouvez remonter vos solutions de stockage externes. Pour plus d'informations sur la configuration de l'espace de stockage externe, voir *Offboard Storage Guide*.

Procédure

1. Redémarrez le dispositif QRadar et sélectionnez **Réinstallation d'usine**.
2. Entrez `flatten` ou `retain`.

   Le programme d'installation partitionne et reformate le disque dur, installe le système d'exploitation, puis réinstalle le produit QRadar. Vous devez attendre que le processus de mise à plat ouretain soit terminé. Ce processus peut prendre plusieurs minutes. Une fois le processus terminé, une confirmation s'affiche.
3. Entrez `SETUP`.
4. Connectez-vous comme utilisateur root.
5. Assurez-vous que le contrat de licence d'utilisateur final (EULA) est affiché.

   Conseil : Appuyez sur la barre d'espacement pour avancer dans le document.
6. Pour les installations de QRadar Console, sélectionnez le modèle d'ajustement **Enterprise**.
7. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.
8. Appliquez votre clé de licence.
   a. Connectez-vous à QRadar :

      `https://`*`Adresse_IP_QRadar`*

      Le nom d'utilisateur par défaut est `admin`. Le mot de passe est celui du compte de l'utilisateur root.
   b. Cliquez sur **Login To QRadar**.
   c. Cliquez sur l'onglet **Admin**.
   d. Dans le volet de navigation, cliquez sur **Configuration système**.
   e. Cliquez sur l'icône **Gestion du système et de la licence**.
   f. Dans la zone de liste **Afficher**, sélectionnez **Licences**, puis téléchargez votre clé de licence.
   g. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.
   h. Dans la liste de systèmes, sélectionnez un système et cliquez sur **Allouer un système à la licence**.

Chapitre 7. Configuration d'une installation de QRadar

Installez IBM Security QRadar "en mode silencieux" ou effectuez une installation automatisée.

Avant de commencer

Vous devez disposer du système d'exploitation Red Hat Enterprise Linux v6.8 et de l'image ISO de QRadar version 7.2.8.

Procédure

1. Placez RHEL sur l'hôte sur lequel vous souhaitez installer QRadar. Pour plus d'informations, voir «Installation de RHEL sur votre propre dispositif», à la page 23.
2. En tant que superutilisateur, utilisez SSH pour vous connecter à l'hôte sur lequel installer QRadar.
3. Sur l'hôte sur lequel vous souhaitez installer QRadar, accédez au répertoire racine et créez un fichier `AUTO_INSTALL_INSTRUCTIONS`, qui contient le contenu suivant :

   ```
   timezone=GMT
   sectempl=Enterprise
   date={<date_données>}
   ntpserver={<nom_serveur_ntp>}
   ntpsync=0
   timechoice=manual
   nicid={<identificateur_NIC_pour_lequel_l'adresse_IP_est_définie>}
   management_iface={<identificateur_interface_gestion>}
   box_ip={<adresse_IP_dispositif>}
   ip_v6=
   netmask={<masque_réseau_dispositif>}
   ipverchoice={<IPv4_ou_IPv6>}
   gateway_v6=
   hostname={<nom_hôte>}
   pdns={<serveur_dns_principal>}
   bdns={<serveur_dns_secondaire>}
   newkey={<clé_activation>}
   defpass={<defpass>}
   isconsole={<console_is>}
   setuptypechoice=normal
   is_ha_appl=0
   isconstandby=yes
   smtpname=localhost
   ```

   Remplacez les paramètres de configuration du fichier par ceux adaptés à votre environnement.

   Important : Vérifiez que le fichier `AUTO_INSTALL_INSTRUCTIONS` n'a aucune extension (.txt ou .doc, par exemple). L'installation n'aboutit pas si le fichier a une extension.

Paramètre	Description
timezone	Fuseau horaire : GMT, AST, EST, PST, etc.
sectempl	Modèle de sécurité : Enterprise ou Logger (pour un gestionnaire de journaux)
date	Date au format AAAA/MM/JJ.

Paramètre	Description
ntpserver	Nom du serveur NTP
ntpsync	Entrez `1` pour établir une synchronisation avec le serveur NTP et `0` pour ne pas établir de synchronisation.
timechoice	Indiquez `manual` pour entrer la date manuellement ou `server` pour que la date soit définie à l'aide du protocole NTP.
nicid	Identificateur de la carte d'interface réseau : eth0, eth1, etc.
management_iface	Identificateur de l'interface de gestion : eth 0, eth1, etc.
box_ip	Adresse IP de l'installation QRadar.
ip_v6	Entrez l'adresse IPv6 pour l'installation QRadar, si nécessaire.
netmask	Masque de réseau pour l'installation.
ipverchoice	IPv4 ou IPv6
gateway_v6	Adresse IPv6 pour la passerelle, si nécessaire.
hostname	Nom de votre système QRadar.
pdns	Serveur DNS principal.
bdns	Serveur DNS secondaire.
newkey	Clé d'activation de l'installation QRadar.
defpass	Valeur sur laquelle définir le mot de passe root.
isconsole	Entrez `Y` s'il s'agit d'une console et `N` dans les cas contraires.
setuptypechoice	Entrez `normal` pour une installation normale ou `recovery` pour une installation de récupération à haute disponibilité.
is_ha_appl	Entrez `0` s'il ne s'agit pas d'un dispositif haute disponibilité. Entrez `1` s'il s'agit d'un dispositif haute disponibilité.
isconstandby	Entrez `0` si l'installation ne s'effectue pas sur une console à haute disponibilité en veille et `1` dans le cas contraire.
smtpname	Entrez le nom SMTP, tel `localhost`.

4. En utilisant un programme SFTP, tel WinSCP, copiez l'élément ISO QRadar sur l'hôte où vous souhaitez installer QRadar.
5. A l'aide d'un programme comme WinSCP, copiez l'image ISO de RHEL v6.8 sur l'hôte sur lequel vous souhaitez installer QRadar.
6. Sur l'hôte où vous effectuez l'installation, créez un répertoire `/media/cdrom` en utilisant la commande suivante :

   ```
   mkdir /media/cdrom
   ```

7. Créez un répertoire `/media/redhat` sur l'hôte en utilisant la commande suivante :

   ```
   mkdir /media/redhat
   ```

8. Montez l'élément ISO QRadar en utilisant la commande suivante :

```
mount -o loop <qradar.iso> /media/cdrom
```

9. Montez l'élément ISO RHEL en utilisant la commande suivante :
```
mount -o loop <RHEL.iso> /media/redhat
```
10. Exécutez la configuration QRadar en utilisant la commande suivante :
```
/media/cdrom/setup
```

Chapitre 8. Présentation du déploiement de QRadar dans un environnement cloud

Vous pouvez installer des instances du logiciel IBM Security QRadar sur un serveur cloud qui est hébergé par Amazon Web Service. Pour établir des communications sécurisées entre des instances sur site et des instances cloud de QRadar, vous devez configurer une connexion VPN. Vous pouvez configurer une connexion OpenVPN ou utiliser une autre méthode, comme une infrastructure VPN de fournisseur de cloud.

Important : Assurez-vous que les conditions requises ci-dessous sont remplies pour éviter que les données de sécurité ne soient compromises :

- Définition d'un mot de passe root fort.
- Autorisations de connexions spécifiques uniquement aux ports 443 (https), 22 (ssh), 1000 (webmin) et 1194 (UDP, TCP pour OpenVPN).

Configurez QRadar pour le cloud en respectant l'ordre suivant :

1. Installez QRadar sur Amazon Web Service (AWS).
2. Pour le cloud et les hôtes sur site, définissez le rôle suivant :
   - Noeud final de serveur d'un tunnel VPN.
   - Noeud final de client d'un tunnel VPN.
   - Hôte membre qui route le trafic destiné au tunnel VPN via le noeud final VPN local.
   - Aucun, s'il s'agit d'un hôte qui n'a pas besoin de communiquer avec les hôtes de l'autre côté du tunnel VPN.
3. Confirmez que les paramètres de pare-feu de QRadar protègent la sécurité de votre réseau.

Configuration d'un hôte QRadar dans Amazon Web Service

Configurez une connexion sécurisée entre des instances sur site et des instances Amazon Web Services (AWS) d'IBM Security QRadar.

Avant de commencer

1. Configurez une paire de clés sur AWS.
2. Créez une instance Amazon EC2 qui répond aux exigences suivantes :

Tableau 14. Instance AWS requise

Conditions requises	Valeur
Image	`RHEL-6.8_HVM_GA-20160503-x86_64-1-Hourly2-GP2`, trouvée dans **Community AMIs**
Type d'instance	m4.2xlarge
Stockage	Trois disques : 1 volume de 200 Go 2 volumes de 2 To

Tableau 14. Instance AWS requise (suite)

Conditions requises	Valeur
Groupe de sécurité	Adresses IP de la liste, avec les ports 22 et 443 ouverts.

Important : Les commandes citées dans cette procédure sont fournies à titre d'exemples. Les valeurs des commandes peuvent varier en fonction des déploiements.

La clé d'instance AWS est obligatoire pour se connecter à l'instance avec SSH.

XFS n'est pas pris en charge sur les charges RedHat Enterprise Linux (RHEL) v6.8 fournies par AWS. Utilisez ext4.

Important : La haute disponibilité n'est pas prise en charge sur les installations QRadar AWS.

Procédure

1. Entrez la commande suivante pour vous connecter à l'instance AWS en utilisant la paire de clés que vous avez créée lors de la configuration de l'instance :

   ```
   ssh -i <votre_clé>.pem ec2-user@<adresse_IP_publique>
   ```

2. Entrez dans l'interpréteur de commandes racine de l'instance AWS à l'aide de la commande suivante :

   ```
   sudo su -
   ```

   Pour revenir à l'interpréteur de commandes racine, vous devez entrer la commande `sudo su -` chaque fois que vous vous reconnectez à l'instance AWS pour revenir au shell root.

3. Déterminez l'unité que vous souhaitez configurer :

   a. Entrez la commande `lsblk` pour afficher les détails de l'unité.

   ```
   # lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0  200G  0 disk
   └─xvda1 202:1    0  200G  0 part /
   xvdb    202:16   0    2T  0 disk
   xvdc    202:32   0    2T  0 disk
   ```

   b. Recherchez l'unité qui n'a pas de partitions et a l'espace de stockage requis.

   Une fois que vous avez trouvé les unités par bloc, exportez le nom et les données d'unité en tant que variables d'environnement à utiliser dans les étapes suivantes. Pour l'exemple précédent, vous devez entrer les commandes suivantes :

   ```
   export device_name=/dev/xvdc
   export device_data=/dev/xvdb
   ```

4. Pour créer un type de partition pour le disque (libellé), entrez les commandes suivantes :

   ```
   parted -a optimal --script ${nom_unité} -- mklabel gpt
   parted -a optimal --script ${données_unité} -- mklabel gpt
   ```

5. Pour créer ces partitions sur l'unité, entrez les commandes suivantes :

Remarque : Les allocations sont fournies à titre d'exemples. Pour plus d'informations sur les partitions, reportez-vous au manuel *IBM Security QRadar - Guide d'installation*.

```
parted -a optimal --script ${nom_dispositif} -- mkpart swap 0% 30%
parted -a optimal --script ${nom_unité} -- mkpart ext4 30% 60%
parted -a optimal --script ${nom_unité} -- mkpart ext4 60% 100%
parted -a optimal --script ${données_unité} -- mkpart ext4 0% 80%
parted -a optimal --script ${données_unité} -- mkpart ext4 80% 100%
```

6. Pour créer les systèmes de fichiers suivants sur l'unité partitionnée, entrez les commandes suivantes :

```
mkswap -L swap1 ${nom_unité}1
mkfs.ext4 ${nom_unité}2
mkfs.ext4 ${nom_unité}3
mkfs.ext4 ${données_unité}1
mkfs.ext4 ${données_unité}2
```

7. Donnez les noms suivants aux partitions :

```
e2label ${nom_unité}2 /var/log
e2label ${nom_unité}3 /store/tmp
e2label ${données_unité}2 /store/transient
e2label ${données_unité}1 /store
```

8. Dans le fichier /etc/fstab, mettez en commentaire les lignes /dev/*<nom_unité>* /mnt, ou /dev/*<device_data>* /mnt le cas échéant.
9. Entrez les commandes suivantes pour ajouter les entrées obligatoire dans le fichier /etc/fstab :

   Important : Collez les commandes dans un éditeur de texte et supprimez les sauts de ligne avant de copier les commandes dans l'invite de commande.

```
eval `blkid -t LABEL=/store -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab

eval `blkid -t LABEL=/store/transient -o export` ; echo
      UUID=$UUID /store/transient $TYPE defaults,noatime 1 1 >> /etc/fstab

eval `blkid -t LABEL=/var/log -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab

eval `blkid -t LABEL=/store/tmp -o export` ; echo UUID=$UUID /store/tmp
 $TYPE defaults,noatime 1 1 >> /etc/fstab

echo "${nom_dispositif}1 swap swap defaults 0 0" >> /etc/fstab
```

10. Pour créer et monter le répertoire /store, entrez les commandes suivantes :

```
mkdir /store
mount /store
mkdir /store/tmp
mount /store/tmp
mkdir /store/transient
mount /store/transient
cd /var; mv log oldlog; mkdir log; mount / var/log; mv oldlog/* log
```

11. Pour activer la permutation entre les unités, entrez la commande suivante :

```
swapon -a
```

12. Confirmez que la ligne /etc/sysconfig/i18n contient la chaîne suivante, y compris les guillemets :

```
LANG="en_US.UTF-8"
```

13. Pour copier l'image ISO sur l'unité, entrez la commande suivante :

```
scp -i <clé.pem
qradar.iso>
ec2-user@<DNS_public>:qradar.iso
```

14. Pour monter l'image ISO, exécutez les commandes ci-dessous dans le répertoire racine :

```
mkdir /media/cdrom
mount -o loop /home/ec2-user/qradar.iso /media/cdrom
```

15. Configurez les dépendances manquantes en utilisant les commandes suivantes :

    Important : Collez les commandes dans un éditeur de texte et supprimez les sauts de ligne avant de copier les commandes dans l'invite de commande.

    ```
    yum  install -y libxml2 libxml2.i686 audit-libs audit-libs.i686 glibc
    glibc.i686 device-mapper-multipath zlib zlib.i686 libcom_err
    libcom_err.i686 nspr nspr.i686 nss nss.i686 nss-util nss-util.i686
    krb5-libs krb5-libs.i686 keyutils-libs keyutils-libs.i686
    openssl   openssl.i686 httpd-tools httpd-devel httpd mod_ssl keyutils
    keyutils.i686 keyutils-libs keyutils-libs.i686 openldap openldap.i686
    openldap-clients cyrus-sasl-lib cyrus-sasl-lib.i686 pam pam.i686 libgcc
    libgcc.i686 elfutils-libelf  elfutils-libelf.i686
    libstdc++   libstdc++.i686
    ```

    ```
    yum remove php.x86_64 php-cli.x86_64 php-common.x86_64
    php-devel.x86_64 php-imap.x86_64 samba-common samba-winbind-clients
    samba-client samba-winbind
    httpd httpd-tools mod_ssl
    ```

    ```
    sed -i -e "s/plugins=1/plugins=0/" /etc/yum.conf
    ```

16. Pour démarrer le programme d'installation et de configuration, entrez la commande suivante :

    ```
    /media/cdrom/setup
    ```

17. Entrez `Y` lorsque vous êtes invité à accepter une installation sur un matériel non pris en charge.
18. Suivez les invites et exécutez l'assistant d'installation de QRadar.

Configuration des noeuds finaux de serveur pour les installations cloud

Utilisez OpenVPN pour configurer un noeud final de serveur sur le serveur cloud lorsque la console IBM Security QRadar est sur site, et que d'autres noeuds de traitement et de stockage sont installés dans le cloud.

Pourquoi et quand exécuter cette tâche

Un noeud final de serveur requiert les éléments suivants :

- Un fichier de configuration OpenVPN principal.
- Des instructions de routage pour chaque client dans le fichier de configuration du serveur.
- Un fichier de configuration pour chaque client qui enregistre les instructions de routage pour chaque client pouvant se connecter.
- Des règles iptables supplémentaires pour autoriser le réacheminement via le tunnel.
- Le réacheminement IP activé dans le noyau.
- Une autorité de certification personnalisée pour l'émission des certificats utilisées pour authentifier les serveurs et les clients.
- Un certificat de serveur émis par l'autorité de certification locale.

Pour plus d'informations sur les options d'outil OpenVPN, entrez `-h`.

Procédure

1. Pour indiquer le noeud final de serveur, entrez la commande suivante afin de définir le noeud final de serveur dans le cloud.

   ```
   /opt/qradar/bin/vpntool server adresse_IP_hôte_serveur
   adresse_réseau_derrière_VPN
   ```

   Exemple :

   ```
   /opt/qradar/bin/vpntool server 1.2.3.4 5.6.7.8/24
   ```

   Si votre réseau exige le mode TCP au lieu du mode UDP sur vos clients et serveurs, entrez la commande suivante avec vos adresses IP requises :

   ```
   /opt/qradar/bin/vpntool server adresse_IP_hôte_serveur
    adresse_réseau_network_address_derrière_VPN --tcp
   ```

   Après que vous avez défini le noeud final de serveur, VPNtool Server exécute les tâches suivantes :

   - Si l'autorité de certification n'est pas établie, l'autorité de certification est initialisée et la clé ainsi que le certificat d'autorité de certification sont créés.
   - L'autorité de certification locale crée une clé et un certificat qui seront utilisés par ce noeud final de serveur.
   - Les propriétés de configuration sont écrites dans le fichier de configuration VPN.

2. Pour générer et déployer la configuration, entrez la commande suivante :

   ```
   /opt/qradar/bin/vpntool deploy
   ```

   Après que vous avez généré et déployé la configuration, VPNtool Server exécute les tâches suivantes :

   - La configuration de serveur OpenVPN est générée et copiée dans le répertoire `/etc/openvpn`.
   - Le certificat de l'autorité de certification, ainsi que la clé et le certificat du serveur, sont copiés dans l'emplacement standard sous `/etc/openvpn/pki`.
   - Les règles IPtables sont construites et rechargées.
   - Le réacheminement est activé et rendu permanent par la mise à jour du fichier `/etc/sysctl.conf`.

3. Pour démarrer le serveur, entrez la commande suivante :

   ```
   /opt/qradar/bin/enable --now
   ```

   La commande `/opt/qradar/bin/enable --now` crée l'état activé permanent et démarre automatiquement OpenVPN au redémarrage du système.

Configuration des réseaux clients pour les installations cloud

Dans les environnements sur site, utilisez OpenVPN pour configurer un réseau client qui communique avec des noeuds finaux au sein du cloud.

Pourquoi et quand exécuter cette tâche

Un client requiert les éléments suivants :

- Un fichier de configuration OpenVPN principal.
- Des règles iptables pour autoriser le réacheminement via le tunnel.
- Réacheminement IP activé dans le noyau.
- Certificat client émis par l'autorité de certification locale.

Procédure

1. Sur le serveur, informez ce dernier de l'existence du nouveau client, en entrant la commande suivante :

   ```
   /opt/qradar/bin/vpntool addclient <nom config/rôle> <réseau dans la notation CIDR>
   ```

   Exemple : `/opt/qradar/bin/vpntool addclient client1 192.0.2.1/24`

   Pour informer le serveur de l'existence du client, les tâches suivantes doivent être exécutées :

   - Le certificat de l'autorité de certification est copié à un emplacement connu.
   - Le clé et le certificat client du fichier PKCS#12 sont extraits et copiés à des emplacements connus.
   - Les propriétés de configuration du client sont écrites dans le fichier de configuration VPN.

2. Déployez et redémarrez le serveur à l'aide de la commande suivante :

   ```
   /opt/qradar/bin/vpntool deploy
   service openvpn restart
   ```

3. Copiez le fichier de données d'identification client et le fichier de l'autorité de certification générés sur l'hôte QRadar qui est utilisé pour ce noeud final client. Les fichiers se trouvent dans le répertoire `/opt/qradar/conf/vpn/pki` du système qui exécute le serveur VPN et seront nommés `<nom de config/rôle>.p12` et `ca.crt`. Les fichiers peuvent être copiés directement sur le noeud final du client VPN via SCP ou indirectement via une clé USB.

   Exemple :

   ```
   scp root@<adresse_IP>:/opt/qradar/conf/vpn/pki/ca.crt /root/ca.crt
   scp root@<adresse_IP>:/opt/qradar/conf/vpn/pki/client1.p12 /root/client1.p12
   ```

4. Sur le client, configurez l'hôte en tant que client VPN :

   ```
   /opt/qradar/bin/vpntool client <adresse_IP>
   ca.crt client.pk12
   ```

   Si votre réseau exige que vous ne configuriez pas le mode UDP sur vos clients et serveurs, vous pouvez utiliser TCP.

   ```
   /opt/qradar/bin/vpntool client <adresse_IP>
   /root/ca.crt /root/Console.p12 --tcp
   ```

5. Pour générer et déployer la configuration, entrez la commande suivante :

   ```
   /opt/qradar/bin/vpntool deploy
   ```

   La génération et le déploiement de la configuration inclut les étapes suivantes :

   - Le fichier de configuration OpenVPN client est généré et copié à l'emplacement `/etc/openvpn`.
   - Le certificat de l'autorité de certification, ainsi que la clé et le certificat client, sont copiés dans les emplacements standard sous `/etc/openvpn/pki`.
   - Les règles Iptables sont générées et chargées.
   - Le réacheminement est activé et rendu permanent par la mise à jour du fichier `/etc/sysctl.conf`.

6. Pour démarrer le client, entrez la commande suivante :

   ```
   /opt/qradar/bin/enable --now
   ```

   La commande `/opt/qradar/bin/enable --now` crée l'état activé permanent et démarre automatiquement OpenVPN au redémarrage du système.

7. Pour connecter le client via le proxy HTTP, entrez la commande suivante :

   ```
   /opt/qradar/bin/vpntool client <adresse_IP> /root/ca.crt
    /root/Console.p12 --http-proxy= <adresse_IP>:<port>
   ```

- La configuration de proxy est toujours en mode TCP, même si vous n'entrez pas TCP dans la commande.
- Consultez la documentation OpenVPN pour plus de détails sur les options de configuration pour l'authentification de proxy. Ajoutez ces options de configuration au fichier suivant :

  `/etc/openvpn/client.conf`

Configuration d'un membre pour les installations cloud

Utilisez OpenVPN afin d'établir des connexions sécurisées pour les hôtes IBM Security QRadar qui ne sont pas des serveurs ou des clients.

Procédure

Pour joindre un hôte QRadar SIEM au réseau VPN local, de façon à ce qu'il puisse communiquer directement avec les hôtes de l'autre côté du tunnel, utilisez la commande suivante :

```
/opt/qradar/bin/vpntool join <adresse IP du serveur VPN> <notation CIDR du réseau distant>
/opt/qradar/bin/vpntool deploy
```

Chapitre 9. Présentation des noeuds de données

Utilisation des noeuds de données dans votre déploiement IBM Security QRadar.

Les noeuds de données permettent aux déploiements QRadar nouveaux et existants d'ajouter de la capacité de stockage et de traitement à la demande lorsque cela est nécessaire.

Les utilisateurs peuvent échelonner le stockage et la puissance de traitement indépendamment de la collecte de données, ce qui se traduit par un déploiement avec une capacité de stockage et de traitement appropriée. Les noeuds de données sont plug-n-play et peuvent être ajoutés à tout moment à un déploiement. Ils s'intègrent en toute transparence avec le déploiement existant.

L'accroissement des volumes de données dans les déploiements implique une compression des données plus tôt dans le processus. La compression de données ralentit les performances du système car ce dernier doit décompacter les données interrogées pour que l'analyse soit possible. L'ajout de dispositifs de noeud de données à un déploiement vous permet de conserver les données décompactées plus longtemps.

Le déploiement QRadar distribue toutes les nouvelles données entre les processeurs d'événement et de flux et les noeuds de données reliés.

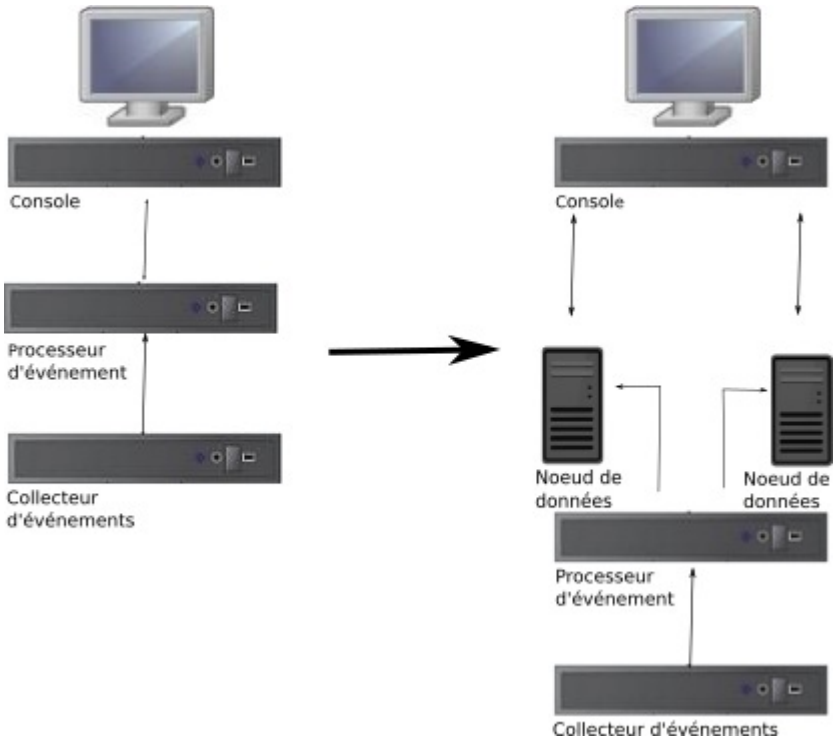

Figure 2. Déploiement QRadar avant et après l'ajout de dispositifs de noeud de données

Mise en cluster

Les noeuds de données ajoutent une capacité de stockage à un déploiement et améliorent également les performances en répartissant entre plusieurs volumes de stockage les données collectées sur un processeur. Lors d'une recherche de données, plusieurs noeuds, autrement dit un "cluster", procèdent à la recherche.Le cluster peut améliorer significativement les performances de la recherche, mais sans nécessiter l'ajout de plusieurs processeurs d'événements.Les noeuds de données multiplient le stockage pour chaque processeur.

Remarque : Vous ne pouvez connecter un noeud de données qu'à un seul processeur à la fois, mais un processeur peut gérer plusieurs noeuds de données.

A propos du déploiement

- Les noeuds de données sont disponibles dans QRadar 7.2.2 et versions suivantes
- Les noeuds de données exécutent des fonctions de recherche et d'analyse similaires aux fonctions des processeurs d'événements et de flux dans un déploiement QRadar. Les opérations sur un cluster sont affectées par le membre le plus lent d'un cluster. Les performances système du noeud de données s'améliorent si les noeuds de données sont redimensionnés de la même façon que les processeurs d'événements et de flux dans un déploiement. Pour faciliter un redimensionnement similaire entre les noeuds de données et les processeurs d'événements et de flux, les noeuds de données sont disponibles à la fois sur les dispositifs centraux XX05 et XX28.
- Les noeuds de données sont disponibles dans trois formats : Logiciel (sur votre propre matériel), Physique et Dispositifs. Vous pouvez combiner plusieurs formats dans un seul cluster.

Bande passante et temps d'attente

Assurez une liaison de 1 Gbit et moins de 10 ms entre les noeuds du cluster. Les recherches renvoyant un grand nombre de résultats nécessitent une bande passante plus large.

Compatibilité

Les noeuds de données sont compatibles avec tous les dispositifs QRadar existants qui ont un composant Processeur d'événements ou de flux, y compris les dispositifs tout en un. Les noeuds de données ne sont pas compatibles avec les dispositifs QRadar Incident Forensics PCAP.

Les noeuds de données prennent en charge la haute disponibilité.

Installation

Les noeuds de données utilisent les réseaux TCP/IP standard et ils n'ont pas besoin d'un matériel de connexion propriétaire ou spécialisé. Installez chaque noeud que vous voulez ajouter à votre déploiement comme si vous installiez tout autre dispositif QRadar. Associez les noeuds de données aux processeurs d'événement ou de flux dans l'éditeur de déploiement QRadar. Voir *IBM Security QRadar Administration Guide*.

Vous pouvez connecter plusieurs noeuds de données à un seul processeur d'événement ou de flux dans une configuration plusieurs à un.

Lorsque vous déployez des paires à haute disponibilité avec des dispositifs de noeud de données, déployez et rééquilibrez les données sur les dispositifs de haute disponibilité avant de synchroniser la paire HD. L'effet combiné du rééquilibrage des données et du processus de réplication utilisé pour la haute disponibilité se traduit par une dégradation significative des performances. Si la haute disponibilité est présente sur les dispositifs existants, dans lesquels sont introduits les noeuds de données, il est également préférable que la connexion haute disponibilité soit interrompue puis rétablie une fois le rééquilibrage du cluster terminé.

Mise hors service

Retirez les noeuds de données de votre déploiement avec l'éditeur de déploiement, comme avec tout autre dispositif QRadar. La mise hors service n'efface pas les données équilibrées sur l'hôte. Les données ne sont pas disponibles dans l'interface utilisateur. Vous pouvez extraire les données pour archivage et redistribution.

Rééquilibrage des données

L'ajout d'un noeud de données à un cluster répartit les données sur chaque noeud de données. Chaque dispositif de noeud de données gère le même taux d'espace disponible. L'ajout de nouveaux noeuds de données à un cluster démarre un rééquilibrage supplémentaire depuis les processeurs d'événement et de flux de cluster afin de parvenir à un usage efficace des disques sur les dispositifs de noeud de données nouvellement ajoutés.

A partir de la version 7.2.3 de QRadar, le rééquilibrage de données est automatique et s'effectue parallèlement à d'autres activités de cluster, telles que les requêtes et la collecte de données. Aucune indisponibilité ne se produit pendant le rééquilibrage de données.

Les noeuds de données ne présentent aucune amélioration des performances du cluster tant que le rééquilibrage des données n'est pas terminé. Le rééquilibrage peut entraîner une dégradation mineure des performances lors des opérations de recherche, mais le traitement et la collecte des données ne sont pas affectés.

Gestion et opérations

Les noeuds de données sont auto-gérés et ne nécessitent aucune intervention de l'utilisateur pour la gestion régulière des opérations normales. QRadar gère les activités, comme les sauvegardes de données, la haute disponibilité et les règles de conservation, pour tous les hôtes, y compris les dispositifs de noeud de données.

Défaillances

Si un noeud de données est défaillant, les autres membres du cluster continuent à traiter les données.

Lorsque le noeud de données défaillant redevient opérationnel, l'équilibrage de données peut avoir lieu pour maintenir une distribution de données sans faille dans le cluster. Le processus normal reprend alors. Au cours de la durée d'immobilisation, les données sur le noeud de données sont indisponibles.

Pour les défaillances graves qui requièrent le remplacement du dispositif ou la réinstallation de QRadar, mettez hors service les noeuds de données du déploiement et remplacez-les à l'aide de la procédure d'installation standard.

Copiez les données non perdues lors de la défaillance sur le nouveau noeud de données avant le déploiement. L'algorithme de rééquilibrage tient compte des données existantes sur un noeud de données et traite uniquement les données collectées pendant la défaillance.

Pour les noeuds de données déployés avec une paire HA, une défaillance matérielle entraîne une basculement, et les opérations se poursuivent normalement.

Concepts associés:

«Composants QRadar», à la page 2
IBM Security QRadar consolide les données d'événement de sources de journal utilisées par des dispositifs et des applications sur votre réseau.

Chapitre 10. Gestion des paramètres réseau

Utilisez `qchange_netsetup script` pour modifier les paramètres réseau de votre système IBM Security QRadar. Les paramètres réseau configurables sont le nom d'hôte, l'adresse IP, le masque de sous-réseau, les adresses DNS, l'adresse IP publique et le serveur de messagerie.

Modification des paramètres réseau dans un système tout-en-un

Vous pouvez modifier les paramètres réseau dans votre système tout-en-un. Un système tout-en-un comporte tous les composants IBM Security QRadar installés sur un système.

Avant de commencer

- Vous devez disposer d'une connexion locale à votre QRadar Console.
- Vérifiez qu'il n'y a aucun changement non déployé.
- Si vous modifiez le nom d'hôte de l'adresse IP d'un boîtier dans le déploiement, vous devez le retirer du déploiement.
- Si ce système fait partie d'une paire HA, vous devez désactiver HA avant de modifier les paramètres réseau.
- Si le système que vous voulez modifier est la console, vous devez supprimer tous les hôtes dans le déploiement avant de poursuivre.

Procédure

1. Connectez-vous comme utilisateur root.
2. Entrez la commande suivante :

   ```
   qchange_netsetup
   ```

3. Pour effectuer la configuration, suivez les instructions de l'assistant.

   Le tableau ci-dessous contient des descriptions et des remarques qui vous seront utiles pour configurer les paramètres réseau.

Tableau 15. Description des paramètres réseaux pour une QRadar Console tout-en-un

Paramètre réseau	**Description**
Protocole IP	`IPv4` or `IPv6`
Nom d'hôte	Nom de domaine qualifié complet
Adresse de serveur DNS secondaire	Facultatif
Adresse IP publique utilisant Network Address Translation (NAT)	Facultatif Permet d'accéder au serveur, généralement à partir d'un autre réseau ou d'Internet. Configuré en utilisant les services Network Address Translation (NAT) sur votre réseau ou dans les paramètres de pare-feu sur votre réseau. (NAT convertit une adresse IP d'un réseau en une autre adresse IP sur un autre réseau.)
Nom du serveur de messagerie	Si vous ne disposez pas d'un serveur de messagerie, utilisez `localhost`.

Une série de messages s'affiche lorsque QRadar traite le modifications demandées. Une fois les modifications demandées traitées, le système QRadar est arrêté et redémarré automatiquement.

Modification des paramètres réseau de QRadar Console dans un déploiement multisystème

Pour modifier les paramètres réseau dans un déploiement IBM Security QRadar multisystème, supprimez tous les hôtes gérés, modifiez les paramètres réseau, rajoutez les hôtes gérés, puis réaffectez le composant.

Avant de commencer

- Vous devez disposer d'une connexion locale à votre QRadar Console.

Procédure

1. Pour supprimer les hôtes gérés, connectez-vous à QRadar :

   `https://`*`Adresse_IP_QRadar`*

   Le **nom d'utilisateur** est `admin`.

   a. Cliquez sur l'onglet **Admin**.
   b. Cliquez sur l'icône **Gestion du système et de la licence**.
   c. Sélectionnez l'hôte géré que vous souhaitez supprimer.
   d. Sélectionnez **Actions de déploiement** > **Retirer l'hôte**.
   e. Sous l'onglet **Admin**, cliquez sur **Déployer les changements**.
2. Entrez la commande suivante : `qchange_netsetup`.
3. Pour effectuer la configuration, suivez les instructions de l'assistant.

   Le tableau ci-dessous contient des descriptions et des remarques qui vous seront utiles pour configurer les paramètres réseau.

Tableau 16. Description des paramètres réseau pour un déploiement multisystème de QRadar Console.

Paramètre réseau	Description
Protocole IP	`IPv4` ou `IPv6`
Nom d'hôte	Nom de domaine qualifié complet
Adresse de serveur DNS secondaire	Facultatif
Adresse IP publique utilisant Network Address Translation (NAT)	Facultatif Permet d'accéder au serveur, généralement à partir d'un autre réseau ou d'Internet. Configuré en utilisant les services Network Address Translation (NAT) sur votre réseau ou dans les paramètres de pare-feu sur votre réseau. (NAT convertit une adresse IP d'un réseau en une autre adresse IP sur un autre réseau.)
Nom du serveur de messagerie	Si vous ne disposez pas d'un serveur de messagerie, utilisez `localhost`.

Une fois que vous avez configuré les paramètres d'installation, une série de messages s'affiche. La procédure d'installation peut prendre plusieurs minutes.

4. Pour rajouter et réaffecter de nouveau les hôtes gérés, connectez-vous à QRadar.

   `https://Adresse_IP_QRadar`

   Le **nom d'utilisateur** est `admin`.

   a. Cliquez sur l'onglet **Admin**.
   b. Cliquez sur l'icône **Gestion du système et de la licence**.
   c. Cliquez sur **Actions de déploiement** > **Ajouter l'hôte**.
   d. Pour ajouter un hôte, suivez les instructions de l'assistant.

      Sélectionnez l'option **Conversion d'adresses réseau** afin de configurer une adresse IP publique pour le serveur. Cette adresse IP est une adresse IP secondaire utilisée pour accéder au serveur, généralement à partir d'un autre réseau ou d'Internet. 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. NAT convertit une adresse IP d'un réseau en une autre adresse IP sur un autre réseau.

5. Réaffectez tous les composants à vos hôtes gérés qui ne se trouvent pas dans votre QRadar Console.

   a. Cliquez sur l'onglet **Admin**.
   b. Cliquez sur l'icône **Gestion du système et de la licence**.
   c. Sélectionnez l'hôte que vous souhaitez réaffecter.
   d. Cliquez sur **Actions de déploiement** > **Modifier une connexion d'hôte**.
   e. Entrez l'adresse IP de l'hôte source dans la fenêtre **Modifier une connexion**.

Mise à jour des paramètres réseau après le remplacement d'une carte d'interface réseau

Si vous remplacez la carte système intégrée ou les cartes d'interface réseau autonomes, vous devez mettre à jour les paramètres réseau de IBM Security QRadar pour vous assurer que votre matériel reste fonctionnel.

Pourquoi et quand exécuter cette tâche

Le fichier de paramètres réseau contient deux lignes pour chaque carte d'interface réseau installée et deux lignes pour chaque carte d'interface réseau supprimée. Vous devez supprimer les lignes de la carte d'interface réseau supprimée, puis renommer la carte d'interface réseau que vous avez installée.

Votre fichier de paramètres réseau peut se présenter comme dans l'exemple ci-dessous, où *NAME="eth0"* correspond à la carte d'interface réseau qui a été remplacée et *NAME="eth4"* correspond à la carte d'interface réseau qui a été installée.

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"
```


```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"
```


Procédure

1. Utilisez le protocole SSH pour vous connecter au produit IBM Security QRadar comme utilisateur root.

   Le nom d'utilisateur est `root`.
2. Entrez la commande suivante :

   `cd /etc/udev/rules.d/`
3. Pour modifier le fichier de paramètres réseau, entrez la commande suivante :

   `vi 70-persistent-net.rules`
4. Supprimez la paire de lignes correspondant au remplacement de la carte d'interface réseau : `NAME="eth0"`.
5. Renommez les valeurs `Name=<eth>` de la carte d'interface réseau qui vient d'être installée.

   Exemple : Renommez `NAME="eth4"` en `NAME="eth0"`.
6. Enregistrez le fichier et fermez-le.
7. Entrez la commande suivante : `reboot`.

Chapitre 11. Traitement des incidents

Le traitement des incidents est une approche systématique pour résoudre un problème. L'objectif du traitement des incidents est de déterminer pourquoi quelque chose ne fonctionne pas de la façon escomptée et comment résoudre le problème.

Consultez le tableau ci-dessous pour vous aider ou aider le service clients à résoudre un problème.

Tableau 17. Actions de traitement des incidents dans un but de prévention

Action	Description
Appliquez tous les groupes de correctifs connus, les niveaux de service ou les correctifs temporaires de programme.	Un correctif de produit peut être disponible pour corriger le problème.
Assurez-vous que la configuration est prise en charge.	Vérifiez la configuration logicielle et matérielle requise.
Consultez les codes de message d'erreur en sélectionnant le produit sur le portail du support IBM (http://www.ibm.com/support/entry/portal), puis en entrant le code du message d'erreur dans la zone **Effectuer une recherche dans le support**.	Les messages d'erreur fournissent des informations importantes pour vous aider à identifier le composant qui cause le problème.
Reproduisez le problème pour vous assurer qu'il ne s'agit pas d'une simple erreur.	Si des exemples sont disponibles avec le produit, vous pouvez essayer de reproduire le problème en utilisant les données des exemples.
Vérifiez la structure de répertoire de l'installation et les autorisations des fichiers.	L'emplacement d'installation doit contenir la structure de fichiers et les autorisations de fichier appropriées. Par exemple, si le produit nécessite un accès en écriture aux fichiers journaux, assurez-vous que le répertoire possède l'autorisation appropriée.
Consultez des documentations pertinentes, telles que des notes sur l'édition, des notes techniques, et des documentations de pratiques éprouvées.	Effectuez une recherche dans les bases de connaissances IBM pour déterminer si votre problème est connu, possède une solution de contournement ou s'il a déjà été résolu et documenté.
Examinez le modifications récentes dans votre environnement informatique.	L'installation de nouveaux logiciels peut parfois causer des problèmes de compatibilité.

Si vous devez toujours résoudre les problèmes, vous devez collecter les données de diagnostic. Ces données peuvent être nécessaires pour qu'un représentant du support technique IBM identifie et résolve efficacement un problème et vous aide à résoudre le problème. Vous pouvez également collecter les données de diagnostic et les analyser vous-même.

Concepts associés:

«Composants QRadar», à la page 2
IBM Security QRadar consolide les données d'événement de sources de journal utilisées par des dispositifs et des applications sur votre réseau.

Traitement des incidents liés aux ressources

Les ressources de traitement des incidents sont des sources d'information qui peuvent vous aider à résoudre un problème que vous pouvez rencontrer avec un produit. Bon nombre des liens de ressource fournis peuvent également être affichés dans une courte démonstration vidéo.

Pour afficher la version vidéo, recherchez "traitement des incidents" dans le moteur de recherche Google ou dans la communauté des vidéos YouTube.

Concepts associés:

«Fichiers journaux QRadar», à la page 63
Utilisez les fichiers journaux IBM Security QRadar pour aider à identifier et résoudre les problèmes.

Portail du support

Le portail du support IBM est une vue uniformisée et centralisée de tous les outils et les informations de support technique pour l'ensemble des systèmes, des logiciels et des services IBM.

Utilisez le portail du support IBM pour accéder à toutes les ressources de support IBM à partir d'un seul emplacement. Vous pouvez ajuster les pages pour vous concentrer sur les informations et les ressources dont vous avez besoin pour la prévention des problèmes et leur résolution rapide. Familiarisez-vous avec le portail du support IBM en visionnant les vidéos de démonstration (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

Recherchez le contenu IBM Security QRadar dont vous avez besoin en sélectionnant vos produits sur le portail du support IBM (http://www.ibm.com/support/entry/portal).

Demandes de service

Les demandes de service sont également appelées dossiers de gestion des problèmes. Il existe différentes méthodes pour envoyer les informations de diagnostic au support technique logiciel IBM.

Pour ouvrir une demande de service ou pour échanger des informations avec le support technique, consultez la page Echange d'informations du service de support logiciel IBM avec le support technique (http://www.ibm.com/software/support/exchangeinfo.html). Les demandes de service peuvent également être envoyées directement avec l'outil Demandes de service (http://www.ibm.com/support/entry/portal/Open_service_request) ou l'une de autres méthodes prises en charge décrites en détail dans la page d'informations sur l'échange.

Fix Central

Fix Central fournit les correctifs et les mises à jour pour vos logiciels système, votre matériel et votre système d'exploitation.

Utilisez le menu déroulant pour accéder aux correctifs du produit dans Fix Central (http://www.ibm.com/support/fixcentral). Vous pouvez également consulter le document Découverte de Fix Central (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html).

Bases de connaissances

Vous pouvez souvent trouver des solutions à des problèmes en effectuant une recherche dans les bases de connaissances IBM. Vous pouvez optimiser vos résultats en utilisant les ressources, les outils de support et les méthodes de recherche disponibles.

Utilisez les bases de connaissances pour rechercher des informations utiles.

Notes techniques et APAR

Sur le site IBM Support Portal (http://www.ibm.com/support/entry/portal), vous pouvez rechercher des notes techniques et des APAR (rapports d'incident).

Recherche de bloc masthead IBM

Utilisez la recherche de bloc masthead IBM en entrant votre chaîne de recherche dans la zone **Recherche** dans la partie supérieure des pages ibm.com.

Moteurs de recherche externes

Recherchez du contenu en utilisant un moteur de recherche externe, comme Google, Yahoo ou Bing. Si vous utilisez un moteur de recherche externe, vos résultats sont plus susceptibles d'inclure des informations extérieures au domaine ibm.com. Cependant, vous pouvez parfois trouver des informations de résolution des problèmes concernant des produits IBM dans des groupes de discussion, des forums et des blogs extérieurs au domaine ibm.com.

Conseil : Dans votre recherche, incluez "IBM" et le nom du produit si vous recherchez des informations concernant un produit IBM.

Fichiers journaux QRadar

Utilisez les fichiers journaux IBM Security QRadar pour aider à identifier et résoudre les problèmes.

Vous pouvez consulter les fichiers journaux pour la session active individuellement ou vous pouvez les collecter pour les consulter ultérieurement.

Pour consulter les fichiers journaux de QRadar, suivez la procédure ci-dessous.

1. Pour aider à identifier et à résoudre des erreurs ou des exceptions, consultez les fichiers journaux suivants.
   - `/var/log/qradar.log`
   - `/var/log/qradar.error`
2. Si vous avez besoin de plus d'informations, consultez les fichiers journaux suivants :
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out
   - /var/log/qflow.debug
3. Pour consulter tous les journaux, sélectionnez **Admin** > **Gestion du système et de la licence** > **Actions** > **Collecter les fichiers journaux**.

Concepts associés:

«Traitement des incidents liés aux ressources», à la page 62
Les ressources de traitement des incidents sont des sources d'information qui peuvent vous aider à résoudre un problème que vous pouvez rencontrer avec un produit. Bon nombre des liens de ressource fournis peuvent également être affichés dans une courte démonstration vidéo.

Ports et serveurs courants utilisés par QRadar

IBM Security QRadar requiert que certains ports soient prêts à recevoir des informations des composants QRadar et de l'infrastructure externe. Pour garantir que QRadar utilise les informations de sécurité les plus récentes, il requiert également un accès aux serveurs publics et aux flux RSS.

Communication SSH sur le port 22

Tous les ports utilisés par la console QRadar pour communiquer avec les hôtes gérés peuvent être tunnélisés, par chiffrement, via le port 22 sur SSH.

Pour communiquer de manière sécurisée, la console se connecte aux hôtes gérés en utilisant une session SSH chiffrée. Les sessions SSH sont démarrées depuis la console afin de fournir les données à l'hôte géré. Par exemple, QRadar Console peut démarrer plusieurs sessions SSH sur les dispositifs du processeur d'événement pour une communication sécurisée. Cette communication peut inclure les ports tunnélisés sur SSH, comme des données HTTPS pour le port 443 et des données de requête Ariel pour le port 32006. IBM Security QRadar QFlow Collector utilisant un chiffrement peut initier des sessions SSH sur les dispositifs Flow Processor qui ont besoin de données.

Ports ouverts non requis par QRadar

Vous pouvez trouver des ports ouverts supplémentaires dans les situations suivantes :

- Lorsque vous installez QRadar sur votre propre matériel, vous pouvez rencontrer des ports ouverts qui sont utilisés par des services, des démons, et des programmes inclus dans Red Hat Enterprise Linux.
- Lorsque vous montez ou exportez un partage de fichiers réseau, vous pouvez rencontrer des ports affectés dynamiquement car requis pour les services RPC, tels que `rpc.mountd` et `rpc.rquotad`.

Utilisation du port QRadar

Examinez la liste des ports usuels utilisés par les services et les composants IBM Security QRadar pour communiquer au sein du réseau. Vous pouvez utiliser cette liste pour déterminer quels ports doivent être ouverts dans votre réseau. Vous pouvez, par exemple, déterminer quel port doit être ouvert pour que QRadar Console communique avec des processeurs d'événement distants.

Interrogation WinCollect à distance

Les agents WinCollect qui interrogent à distances d'autres systèmes d'exploitation Microsoft Windows peuvent nécessiter des affectations de ports supplémentaires.

Pour plus d'informations, reportez-vous au manuel IBM Security QRadar WinCollect - *Guide d'utilisation*.

Ports d'écoute QRadar

Le tableau suivant répertorie les ports QRadar ouverts à l'état `Ecoute`. Les ports `Ecoute` ne sont valides que lorsqu'iptables est activé sur votre système. Sauf mention contraire, les informations sur le numéro de port affecté s'appliquent à tous les produits QRadar.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar

Port	Description	Protocole	Direction	Conditions requises
22	SSH	TCP	Trafic bidirectionnel entre QRadar Console et tous les autres composants.	Accès de gestion à distance. Ajout d'un système distant en tant qu'hôte géré. Protocoles de source de journal pour extraction de fichiers depuis des périphériques externes, par exemple le protocole de fichier journal. Utilisateurs recourant à l'interface de ligne de commande pour communiquer avec la console depuis leur ordinateur de bureau. Haute disponibilité (HA).
25	SMTP	TCP	De tous les hôtes gérés à la passerelle SMTP.	Courriers électronique depuis QRadar vers une passerelle SMTP. Remise de messages d'erreur et d'avertissement à une adresse de contact électronique d'administration.
37	rdate (heure)	UDP/ TCP	Tous les systèmes vers QRadar Console. QRadar Console vers le serveur NTP ou rdate.	Synchronisation d'horloge entre QRadar Console et les systèmes gérés.
111	Associateur de port	TCP/ UDP	Hôtes gérés communiquant avec le QRadar Console. Utilisateurs se connectant à QRadar Console.	Appels de procédure distante aux services requis, tels que NFS (Network File System).

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
Port 135 et ports alloués dynamiquement au-delà du port 1024 pour les appels RPC	DCOM	TCP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les composants QRadar Console ou les collecteurs d'événement IBM Security QRadar utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter. **Remarque :** DCOM alloue généralement une plage de ports aléatoire pour la communication. Vous pouvez configurer les produits Microsoft Windows afin d'utiliser un port spécifique. Pour plus d'informations, reportez-vous à la documentation Microsoft Windows.
137	Service de noms Windows NetBIOS	UDP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
138	Service de datagramme Windows NetBIOS	UDP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
139	Service de session Windows NetBIOS	TCP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
162	NetSNMP	UDP	Hôtes gérés QRadar se connectant à QRadar Console. Sources de journal externes vers QRadar Event Collectors.	Port UDP pour le démon NetSNMP à l'écoute de communications (v1, v2c et v3) depuis des sources de journal externes. Le port n'est ouvert que si l'agent SNMP est activé.
199	NetSNMP	TCP	Hôtes gérés QRadar se connectant à QRadar Console. Sources de journal externes vers QRadar Event Collectors.	Port TCP pour le démon NetSNMP à l'écoute de communications (v1, v2c et v3) depuis des sources de journal externes. Le port n'est ouvert que si l'agent SNMP est activé.
427	Service Location Protocol (SLP)	UDP/ TCP		Integrated Management Module utilise le port pour rechercher des services sur un réseau local.
443	Apache/HTTPS	TCP	Trafic bidirectionnel pour les communications sécurisées depuis tous les produits vers QRadar Console.	Téléchargement des configurations sur les hôtes gérés depuis QRadar Console. Hôtes gérés QRadar se connectant à QRadar Console. Utilisateurs devant pouvoir se connecter à QRadar. QRadar Console qui gère et fournit des mises à jour de la configuration aux agents WinCollect.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
445	Microsoft Directory Service	TCP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant Microsoft Security Event Log Protocol et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les agents Adaptive Log Exporter et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
514	Syslog	UDP/ TCP	Dispositifs réseau externes fournissant des événements syslog TCP et utilisant le trafic bidirectionnel Dispositifs réseau externes fournissant des événements syslog UDP et utilisant le trafic unidirectionnel Trafic syslog interne depuis les hôtes QRadar vers QRadar Console.	Sources de journal externes envoyant des données d'événement aux composants QRadar. Le trafic Syslog inclut les agents WinCollect, les collecteurs d'événements et les agents Adaptive Log Exporter capables d'envoyer des événements UDP ou TCP à QRadar.
762	Démon de montage (mountd) Network File System (NFS)	TCP/ UDP	Connexions entre QRadar Console et le serveur NFS.	Démon de montage NFS (Network File System) traitant les demandes de montage d'un système de fichiers à un emplacement spécifié.
1514	Syslog-ng	TCP/ UDP	Connexion entre le composant local collecteur d'événements et le composant local processeur d'événement au démon syslog-ng pour journalisation.	Port de journalisation interne pour syslog-ng.
2049	NFS	TCP	Connexions entre QRadar Console et le serveur NFS.	Protocole NFS (Network File System) pour partage de fichiers ou de données entre les composants.
2055	Données NetFlow	UDP	De l'interface de gestion sur la source du flux (en général, un routeur) au IBM Security QRadar QFlow Collector.	Datagramme NetFlow à partir de composants, comme des routeurs.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
2375	Port de commande Docker	TCP	Communications internes. Ce port n'est pas disponible depuis l'extérieur.	Utilisé pour gérer les ressources d'infrastructure d'application QRadar.
3389	Remote Desktop Protocol (RDP) et Ethernet sur USB sont activés	TCP/ UDP		Si le système d'exploitation Microsoft Windows est configuré pour prise en charge de RDP et d'Ethernet over USB, un utilisateur peut ouvrir une session sur le serveur via le réseau de gestion. Cela signifie que le port par défaut pour RDP, le port 3389, doit être ouvert.
3900	Port de présence distante de Integrated Management Module	TCP/ UDP		Utilisez ce port pour interagir avec la console QRadar par le biais de Integrated Management Module.
4333	Port de redirection	TCP		Ce port est affecté comme port de redirection pour les demandes du protocole de résolution d'adresse (ARP) dans la résolution des infractions QRadar.
5432	Postgres	TCP	Communication pour l'hôte géré utilisé pour accéder à l'instance de base de données locale.	Requis pour mettre à disposition des hôtes gérés depuis l'onglet **Admin**.
6514	Syslog	TCP	Les dispositifs réseau externes qui fournissent des événements syslog TCP chiffrés utilisent un trafic bidirectionnel.	Sources de journal externes envoyant des données d'événement chiffrées aux composants QRadar.
6543	Signal de présence haute disponibilité	TCP/ UDP	Trafic bidirectionnel entre l'hôte secondaire et l'hôte principal dans un cluster HD.	Requête ping de signal de présence d'un hôte secondaire vers un hôte principal dans un cluster HD pour détecter un échec matériel ou réseau.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
7676, 7677 et quatre ports associés de façon aléatoire au-delà du port 32000.	Connexions de messagerie (IMQ)	TCP	Communications de file d'attente de message entre les composants sur un hôte géré	Courtier de file d'attente de messages pour les communications entre les composants sur un hôte géré. **Remarque :** Vous devez autoriser l'accès à ces ports depuis la console QRadar pour les hôtes non chiffrés. Les ports 7676 et 7677 sont des ports TCP statiques et quatre connexions supplémentaires sont créées sur des ports aléatoires. Pour plus d'informations sur l'identification de ports liés de manière aléatoire, voir «Affichage des associations de ports IMQ», à la page 74.
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799 et 8989.	Ports du serveur JMX	TCP	Communications internes. Ces ports ne sont pas disponibles depuis l'extérieur.	Serveur JMX (Java Management Beans) suivant tous les processus QRadar internes pour exposer les métriques de prise en charge. Ces ports sont utilisés par la prise en charge de QRadar.
7789	Dispositif de bloc répliqué distribué HD	TCP/ UDP	Trafic bidirectionnel entre l'hôte secondaire et l'hôte principal dans un cluster HD.	Architecture de dispositif de bloc répliqué distribué (Distributed Replicated Block Device) utilisée pour maintenir la synchronisation entre hôte primaire et hôte secondaire dans les configurations HD.
7800	Apache Tomcat	TCP	Depuis le collecteur d'événements vers QRadar Console.	Diffusion en temps réel (diffusion en flux) des événements.
7801	Apache Tomcat	TCP	Depuis le collecteur d'événements vers QRadar Console.	Diffusion en temps réel (diffusion en flux) des flux.
7803	Apache Tomcat	TCP	Depuis le collecteur d'événements vers QRadar Console.	Port du moteur de détection d'anomalies.
7804	Générateur QRM Arc	TCP	Communications de contrôle interne entre les processus QRadar et le générateur ARC.	Ce port est utilisé uniquement pour QRadar Risk Manager. Il n'est pas disponible en externe.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
8000	Service de collecte d'événements (ECS)	TCP	Depuis le collecteur d'événements vers QRadar Console.	Port d'écoute pour service de collecte d'événements (ECS) spécifique.
8001	Port du démon SNMP	UDP	Systèmes SNMP externes demandant des informations d'interception SNMP auprès de QRadar Console.	Port d'écoute UDP pour les demandes de données SNMP externes
8005	Apache Tomcat	TCP	Communications internes. Non disponible en externe.	Ouvert pour contrôle de Tomcat. Ce port est lié et n'accepte des connections que depuis l'hôte local.
8009	Apache Tomcat	TCP	Depuis le processus du démon HTTP (HTTPd) vers Tomcat.	Connecteur Tomcat lorsque la demande est utilisée et substituée par proxy au service Web
8080	Apache Tomcat	TCP	Depuis le processus du démon HTTP (HTTPd) vers Tomcat.	Connecteur Tomcat lorsque la demande est utilisée et substituée par proxy au service Web
8413	Agents WinCollect	TCP	Trafic bidirectionnel entre l'agent WinCollect et QRadar Console.	Ce trafic est généré par l'agent WinCollect et la communication est chiffrée. Requis pour fournir des mises à jour de la configuration à l'agent WinCollect et pour utiliser WinCollect en mode connecté.
8844	Apache Tomcat	TCP	Unidirectionnel de QRadar Console vers le dispositif qui exécute le processeur QRadar Vulnerability Manager.	Utilisé par Apache Tomcat pour lire les flux RSS à partir de l'hôte qui exécute le processeur QRadar Vulnerability Manager.
9090	Base de données et serveur XForce IP Reputation	TCP	Communications internes. Non disponible en externe.	Communications entre les processus QRadar et la base de données XForce Reputation IP.
9913, plus un port affecté dynamiquement	Conteneur d'application Web	TCP	Communication RMI (Remote Method Invocation) Java bidirectionnelle entre machines virtuelles Java	Lorsque l'application Web est enregistrée, un port supplémentaire est affecté dynamiquement.
9995	Données NetFlow	UDP	De l'interface de gestion sur la source du flux (en général, un routeur) au QRadar QFlow Collector.	Datagramme NetFlow à partir de composants, comme des routeurs.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
9999	Processeur IBM Security QRadar Vulnerability Manager	TCP	Unidirectionnel depuis le scanner vers le dispositif exécutant le processeur QRadar Vulnerability Manager	Utilisé pour les informations de la commande QRadar Vulnerability Manager (QVM). QRadar Console se connecte à ce port sur l'hôte qui exécute le processeur QRadar Vulnerability Manager. Ce port n'est utilisé que si QVM est activé.
10000	Interface d'administration du système QRadar basée sur le Web	TCP/ UDP	Systèmes des ordinateurs de bureau des utilisateurs vers tous les hôtes QRadar.	Dans QRadar version 7.2.5 et antérieure, ce port est utilisé pour les modifications sur le serveur, comme le mot de passe racine des hôtes et l'accès au pare-feu. Le port 10000 est désactivé dans version 7.2.6.
10101, 10102	Commande de signal de présence	TCP	Trafic bidirectionnel entre le noeud à haute disponibilité principal et le noeud à haute disponibilité secondaire.	Requis pour s'assurer que les noeuds HD sont toujours actifs.
15433	Postgres	TCP	Communication pour l'hôte géré utilisé pour accéder à l'instance de base de données locale.	Utilisé pour la configuration et le stockage QRadar Vulnerability Manager (QVM). Ce port n'est utilisé que si QVM est activé.
23111	Serveur Web SOAP	TCP		Port SOAP du serveur Web pour le service de collecte d'événements (ECS).
23333	Emulex Fibre Channel	TCP	Systèmes des ordinateurs de bureau des utilisateurs se connectant aux dispositifs QRadar via une carte Fibre Channel.	Service elxmgmt (Emulex Fibre Channel HBAnywhere Remote Management).
32004	Transfert d'événements normalisés	TCP	Trafic bidirectionnel entre les composants QRadar.	Données d'événement normalisées communiquées à partir d'une source hors site ou entre des QRadar Event Collectors
32005	Flux de données	TCP	Trafic bidirectionnel entre les composants QRadar.	Port de communication du flux de données entre QRadar Event Collectors sur des hôtes gérés distincts.

Tableau 18. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Conditions requises
32006	Requêtes Ariel	TCP	Trafic bidirectionnel entre les composants QRadar.	Port de communication entre le serveur proxy Ariel et le serveur de requêtes Ariel.
32007	Données en infraction	TCP	Trafic bidirectionnel entre les composants QRadar.	Evénements et flux impliqués dans une infraction ou dans une corrélation globale.
32009	Données d'identité	TCP	Trafic bidirectionnel entre les composants QRadar.	Données d'identité communiquées entre le service d'informations de vulnérabilité passif (VIS) et le service de collecte d'événements (ECS)
32010	Port source d'écoute du flux	TCP	Trafic bidirectionnel entre les composants QRadar.	Port d'écoute du flux pour collecte de données à partir des collecteurs QRadar QFlow
32011	Port d'écoute Ariel	TCP	Trafic bidirectionnel entre les composants QRadar.	Port d'écoute Ariel pour les recherches dans la base de données, les informations de progression et les autres commandes associées.
32000-33999	Flux de données (flux, événements, contexte du flux)	TCP	Trafic bidirectionnel entre les composants QRadar.	Flux de données, tels qu'événements, flux, contexte du flux et requêtes de recherche d'événement
40799	Données PCAP	UDP	Depuis des dispositifs Juniper Networks SRX Series vers QRadar.	Collecte de données de capture de paquets entrants (PCAP) à partir de dispositif Juniper Networks SRX Series. **Remarque :** La capture de paquets sur votre dispositif peut utiliser un autre port. Pour plus d'informations sur la configuration de la capture de paquets, consultez la documentation des dispositifs Juniper Networks SRX Series.
ICMP	ICMP		Trafic bidirectionnel entre l'hôte secondaire et l'hôte principal dans un cluster HD.	Test à l'aide du protocole ICMP (Internet Control Message Protocol) de la connexion réseau entre l'hôte secondaire et l'hôte principal dans un cluster HD.

Affichage des associations de ports IMQ

Plusieurs ports utilisés par IBM Security QRadar affectent des numéros de port aléatoires supplémentaires. Par exemple, Message Queues (IMQ) ouvre des ports aléatoires pour la communication entre les composants sur un hôte géré. Vous pouvez afficher les affectations de port aléatoires pour IMQ en utilisant Telnet pour vous connecter à l'hôte local et en effectuant une recherche sur le numéro de port.

Les associations de port aléatoires ne sont pas des numéros de port statiques. En cas de redémarrage d'un service, les ports générés pour ce service sont réaffectés et un nouvel ensemble de numéros de port est affecté au service.

Procédure

1. En utilisant Secure Shell (SSH), connectez-vous à QRadar Console en tant qu'utilisateur root.
2. Pour afficher une liste des ports associés pour la connexion de messagerie IMQ, entrez la commande suivante :

   `telnet localhost 7676` Les résultats de la commande Telnet peuvent être semblables à ceci :

   ```
   [root@domain ~]# telnet localhost 7676
   Trying 127.0.0.1...
   Connected to localhost.
   Escape character is '^]'.
   101 imqbroker 4.4 Update 1
   portmapper tcp PORTMAPPER 7676
   [imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=3632530563278693376]
   cluster_discovery tcp CLUSTER_DISCOVERY 44913
   jmxrmi rmi JMX 0 [url=service:jmx:rmi://domain.ibm.com/stub/<urlpath>]
   admin tcp ADMIN 43691
   jms tcp NORMAL 7677
   cluster tcp CLUSTER 36615
   ```

   La sortie de la commande Telnet montre 3 des 4 ports TCP aléatoires à numéro élevé destinés à IMQ. Le quatrième port, qui ne figure pas dans la sortie ci-dessus, est un port JMX Remote Method Invocation (RMI) disponible par l'URL JMX qui y figure.

   Un refus de la connexion Telnet indique qu'IMQ n'est pas en cours d'exécution. Dans ce cas, il est probable que le système est en cours de démarrage ou d'arrêt, ou que les services ont été fermés manuellement.

Recherche des ports utilisés par QRadar

Utilisez la commande **netstat** pour déterminer les ports utilisés sur la Console IBM Security QRadar ou l'hôte géré. Utilisez la commande **netstat** pour afficher tous les ports d'écoute et les ports définis sur le système.

Procédure

1. Avec SSH, connectez-vous à votre QRadar Console comme utilisateur root.
2. Pour afficher toutes les connexions actives et tous les ports TCP et UDP écoutés par l'ordinateur, entrez la commande suivante :

   ```
   netstat -nap
   ```

3. Pour rechercher des informations spécifique dans la liste des ports netstat, entrez la commande suivante :

   ```
   netstat -nap | grep port
   ```

   Exemples :

- Pour afficher tous les ports qui correspondent à 199, entrez la commande suivante :

```
netstat
-nap | grep
199
```

- Pour afficher les informations sur tous les ports d'écoute, entrez la commande suivante :

```
netstat
-nap | grep LISTEN
```

Serveurs QRadar publics

Pour vous procurer les informations de sécurité les plus récentes, IBM Security QRadar doit pouvoir accéder à un certain nombre de serveurs publics et de flux RSS.

Serveurs publics

Tableau 19. Serveurs publics auxquels QRadar doit pouvoir accéder. Ce tableau décrit les adresses IP ou les noms d'hôtes auxquels accède QRadar.

Adresse IP ou nom d'hôte	Description
194.153.113.31	Scanner de zone démilitarisée IBM Security QRadar Vulnerability Manager
194.153.113.32	Scanner de zone démilitarisée QRadar Vulnerability Manager
qmmunity.q1labs.com	Serveur de mise à jour QRadar automatique. Pour plus d'informations sur les serveurs de mise à jour automatique, voir www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).
www.iss.net	Tableau de bord du Centre d'informations sur les menaces Internet d'IBM Security X-Force Threat Intelligence
update.xforce-security.com	Serveur de mise à jour du Flux de menaces X-Force
license.xforce-security.com	Serveur de licences du Flux de menaces X-Force

Flux RSS pour les produits QRadar

Tableau 20. Flux RSS. La liste suivante répertorie les exigences de flux RSS utilisés par QRadar. Copiez ces URL dans un éditeur de texte et supprimez les sauts de page avant de les coller dans un navigateur.

Titre	URL	Exigences
Security Intelligence	http://feeds.feedburner.com/SecurityIntelligence	QRadar et connexion Internet
Security Intelligence Vulns / Threats	http://securityintelligence.com/topics/vulnerabilities-threats/feed	QRadar et connexion Internet

Tableau 20. Flux RSS (suite). La liste suivante répertorie les exigences de flux RSS utilisés par QRadar. Copiez ces URL dans un éditeur de texte et supprimez les sauts de page avant de les coller dans un navigateur.

Titre	URL	Exigences
IBM My Notifications	http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid= feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid= S14b5f284d32&feeder.subdefkey=swgother&feeder.maxfeed=25	QRadar et connexion Internet
Nouvelles sur la sécurité	http://*Adresse_IP_processeur_QVM* :8844/rss/research/news.rss	Déploiement du processeur IBM Security QRadar Vulnerability Manager
Consignes de sécurité	http://*Adresse_IP_processeur_QVM* :8844/rss/research/advisories.rss	Déploiement du processeur QRadar Vulnerability Manager
Dernières vulnérabilités publiées	http://*Adresse_IP_processeur_QVM* :8844/rss/research/vulnerabilities.rss	Déploiement du processeur QRadar Vulnerability Manager
Analyses effectuées	http://*Adresse_IP_processeur_QVM* :8844/rss/scanresults/completedScans.rss	Déploiement du processeur QRadar Vulnerability Manager
Analyses en cours	http://*Adresse_IP_processeur_QVM* :8844/rss/scanresults/runningScans.rss	Déploiement du processeur QRadar Vulnerability Manager

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE 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 tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

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

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

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

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

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

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

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

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

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

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

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

Marques

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

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.

Dispositions relatives à la documentation du produit

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

Applicabilité

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

Utilisation personnelle

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

Utilisation commerciale

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

Droits

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

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

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

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

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

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

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

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