IBM Security QRadar
Version 7.3.0

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 69.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.0 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 pour votre commande du dispositif auprès d'IBM! Il est vivement recommandé d'appliquer le dernier niveau de maintenance à votre dispositif afin d'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 (en anglais) (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 (en anglais) (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Instructions relatives aux bonnes pratiques de sécurité

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

L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

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

Chapitre 1. 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, consultez le document *IBM Security QRadar High Availability Guide*.

Nouveautés de QRadar version 7.3.0

IBM Security QRadar version 7.3.0 utilise Red Hat Enterprise Linux (RHEL) V7.3, supprime les clés d'activation, introduit un pool de licences partagé pour la gestion de la capacité d'événements par seconde (EPS) et de flux par minute (FPM), et permet l'amélioration des performances.

Avantages de RHEL V7.3

RHEL V7.3 rend QRadar plus sécurisé. RHEL V7.3 prend également en charge la gestion de volume logique, qui offre une fonctionnalité de partitionnement de disque avancée et flexible. Le gestionnaire de volume logique vous permet de créer des partitions, de les redimensionner et de regrouper des clusters de stockage. Vous disposez, par exemple, d'un dispositif virtuel QRadar tout-en-un. Vous avez besoin de davantage d'espace disque local pour stocker les événements pendant plus longtemps. Vous pouvez étendre la partition `/store` en rajoutant un disque.

Les clés d'activation ne sont plus nécessaires

Au cours de l'installation de QRadar version 7.3.0, vous sélectionnez dans une liste le type de dispositif à installer. Dans les versions précédentes, les responsables de l'installation devaient saisir manuellement sa clé d'activation.

Le pool de licences partagé offre une plus grande souplesse

Vous pouvez ajuster votre système en fonction des modifications en répartissant la capacité d'événements par seconde (EPS) et le flux par minute (FPM) sur n'importe quel hôte du déploiement, quel que soit le dispositif auquel la licence a été accordée.

Prenons l'exemple d'un déploiement distribué comportant deux processeurs d'événements, l'un avec 7 500 EPS et l'autre avec 15 000 EPS. Dans QRadar version 7.3.0, l'ensemble des 22 500 EPS font partie du pool de licences partagé. En cas de variation des volumes de données des processeurs d'événement ou lorsque vous ajoutez un hôte géré, vous pouvez répartir la capacité d'EPS.

Pour plus d'informations sur la gestion du pool de licences partagé, consultez le chapitre relatif à la gestion des licences dans *IBM Security QRadar Administration Guide*.

Clés de licence

Une fois IBM Security QRadar installé, vous devez appliquer vos clés 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
Seuil d'événements par seconde (EPS) **Important :** Cette restriction s'applique également à la clé de licence par défaut d'IBM QRadar Log Manager.	5 000
Flux par intervalle	200 000

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 de 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 13
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 matériel», à la page 19
Vous pouvez installer le système d'exploitation Red Hat Enterprise Linux (RHEL) sur votre propre matériel de dispositif afin de l'utiliser avec IBM Security QRadar.

«Installation du logiciel QRadar sur un ordinateur virtuel», à la page 28
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 *Module de gestion intégré - Guide d'utilisation* sur le CD qui accompagne votre dispositif.

Concepts associés:

«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 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, des composants processeur d'événements ou des 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 13
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 matériel», à la page 19
Vous pouvez installer le système d'exploitation Red Hat Enterprise Linux (RHEL) sur votre propre matériel de dispositif afin de l'utiliser avec IBM Security QRadar.

«Installation du logiciel QRadar sur un ordinateur virtuel», à la page 28
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.

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.

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

Tableau 2. 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	54 et 55

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 3
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 :

- Système Linux sur lequel Red Hat Enterprise Linux V7.3
- Apple Mac OS X
- Microsoft Windows

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 sur un système Microsoft Windows

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

Avant de commencer

Vous devez avoir accès aux éléments suivants :

- Une clé USB d'au moins 8 Go
- Un ordinateur de bureau ou un ordinateur portable doté de l'un des systèmes d'exploitation suivants :
  - Windows 10
  - Windows 7
  - Windows 2008R2
  - Windows 2008
  - Windows Vista
  - Windows XP

Pourquoi et quand exécuter cette tâche

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

Procédure

1. Téléchargez le fichier image ISO QRadar à partir de Fix Central (www.ibm.com/support/fixcentral/).
2. Téléchargez l'outil Rufus depuis Rufus Downloads (http://rufus.akeo.ie/downloads/).
3. Insérez la clé USB amorçable dans un port USB de votre ordinateur.
4. Ouvrez Rufus et configurez les propriétés.

Paramètre	Valeur
Partition scheme and target system type	Schéma de partition du MBR pour le BIOS ou l'UEFI
File system	FAT32 (valeur par défaut)
Cluster size	4096 octets (valeur par défaut)

Paramètre	Valeur
Format Options	Sélectionnez les options suivantes : **Quick format** **Create a bootable disk using** **Create extended label and icon files**

5. Cliquez sur l'icône située en regard de la liste déroulante **Create a bootable disc using** et sélectionnez le fichier ISO de QRadar version 7.3.0.
6. Cliquez sur **Start**.
7. Dans la fenêtre **Hybrid image detected**, sélectionnez **Write in DD Image mode** et cliquez sur **OK**.
8. Lorsque l'installation est terminée, retirez en toute sécurité la clé USB de votre ordinateur.

   Important : Lorsque l'image a été enregistrée sur la clé USB, Windows ne reconnaît plus celle-ci. Pour réutiliser la clé USB, recommencez la procédure avec une image ISO quelconque en sélectionnant **Write in ISO Image mode (Recommended)** dans la fenêtre **Hybrid image detected**.

Que faire ensuite

Pour plus d'informations, voir la rubrique décrivant l'installation de QRadar avec un clé USB.

Création d'une clé USB amorçable avec un système Apple Mac OS X

Vous pouvez utiliser un dispositif un ordinateur Apple Mac OS X pour une clé USB amorçable permettant d'installer des logiciels QRadar.

Avant de commencer

Vous devez avoir accès aux éléments suivants :

- Une clé USB d'au moins 8 Go
- Un fichier image ISO de QRadar version 7.3.0 ou version suivante

Pourquoi et quand exécuter cette tâche

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

Procédure

1. Téléchargez le fichier image ISO QRadar à partir de Fix Central (www.ibm.com/support/fixcentral/).
2. Insérez la clé USB amorçable dans un port USB de votre ordinateur.
3. Ouvrez un terminal et tapez la commande suivante pour démonter la clé USB :

   ```
   diskutil unmountDisk /dev/<nom de la clé USB connectée>
   ```

4. Tapez la commande suivante pour placer le fichier ISO QRadar sur votre clé USB :

   ```
   dd if=/<qradar.iso> of=/dev/ r <nom de la clé USB connectée> bs=1m
   ```

Remarque : La lettre «r» devant le nom de la clé USB connectée désigne le mode "raw", qui permet de réduire le temps de transfert. Il n'y a pas d'espace entre la lettre «r» et le nom de la clé USB connectée.

5. Retirez la clé USB de votre système.

Que faire ensuite

Pour plus d'informations, voir la rubrique décrivant l'installation de QRadar avec une clé USB.

Création d'une clé USB amorçable sur un système Red Hat Linux

Vous pouvez utiliser un ordinateur de bureau ou un portable avec Red Hat Enterprise Linux V7.3 pour créer une clé USB amorçable permettant d'installer les logiciels QRadar.

Avant de commencer

Vous devez avoir accès aux éléments suivants :

- Une clé USB d'au moins 8 Go
- Un fichier image ISO de QRadar version 7.3.0 ou version suivante

Pourquoi et quand exécuter cette tâche

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

Procédure

1. Téléchargez le fichier image ISO QRadar à partir de Fix Central (www.ibm.com/support/fixcentral/).
2. Insérez la clé USB amorçable dans un port USB de votre ordinateur.

   Jusqu'à 30 secondes peuvent être nécessaires pour que le système reconnaisse la clé USB.
3. Ouvrez un terminal et tapez la commande suivante pour déterminer le nom de la clé USB :

   ```
   dmesg | grep SCSI
   ```

   Le système affiche les messages générés par les pilotes de la clé. L'exemple suivant indique que le nom de le clé USB connectée est *sdb*.

   ```
   [ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
   ```
4. Tapez les commandes suivantes pour démonter la clé USB :

   ```
   df -h | grep <nom de la clé USB connectée>
   umount /dev/<nom de la clé USB connectée>
   ```
5. Tapez la commande suivante pour placer le fichier ISO QRadar sur votre clé USB :

   ```
   dd if=/<qradar.iso> of=/dev/<nom de la clé USB connectée> bs=512k
   ```
6. Retirez la clé USB de votre système.

Que faire ensuite

Pour plus d'informations, voir la rubrique décrivant l'installation de QRadar avec une 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 écran, sélectionnez **Install Red Hat Enterprise Linux 7.3**.
   - Si vous avez un ordinateur portable avec une connexion série, sélectionnez **Install Red Hat Enterprise Linux 7.3 using Serial console without format prompt** ou **Install Red Hat Enterprise Linux 7.3 using Serial console with format prompt**.
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.

Un Event Collector configuré pour stocker les données et les transmettre à un processeur d'événements lance la transmission en fonction du planning que vous avez défini. Vérifiez que vous disposez d'une largeur de bande suffisante pour la quantité de données collectée, pour permettre au dispositif de respecter le rythme planifié.

Utilisez les méthodes suivantes pour réduire les limitations liées à la bande passante entre les centres de données :

Traitez et envoyez les données aux hôtes du centre de données principal.
Concevez votre déploiement de manière à traiter et à envoyer les données au fur et à mesure de leur collecte aux hôtes du centre de données principal sur lequel réside la console. De la sorte, toutes les demandes de recherche de l'utilisateur interrogent 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 au sein du réseau. La bande de données est utilisée sur les emplacements distants et recherche des données produites dans le centre de données principal, et non pas à un emplacement distant.

N'effectuez pas de recherches impliquant de grands volumes de données sur des connexions à bande passante limitée
Empêchez les utilisateurs d'effectuer des recherches impliquant des grands volumes de données sur des liens dont la bande passante est limitée. La définition de filtres détaillés sur les recherches limite la quantité de données extraites des emplacements distants, et la bande passante nécessaire pour renvoyer les résultats.

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 versions de logiciel pour tous les dispositifs QRadar d'un déploiement doivent être de même version et de 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 matériel requis est installé.
- Vous disposez de la clé de licence requise pour votre dispositif.
- Un clavier et un écran sont connectés au moyen d'une connexion VGA.
- Si vous voulez configurer des interfaces réseau garanties, voir www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).
- Il n'existe aucune licence arrivée à expiration sur la console ou sur les hôtes gérés.

Important : Si vous êtes invité à entrer un nom d'utilisateur et un mot de passe avant le début de l'assistant d'installation, entrez `root` pour le nom d'utilisateur et `password` pour le mot de passe.

Procédure

1. Entrez `root` à l'invite de connexion pour lancer l'assistant d'installation.
2. Acceptez le Contrat de licence utilisateur final.
3. Sélectionnez le type de dispositif :
   - **Appliance Install**
   - **Software Install**
   - **High Availability Appliance**
4. Sélectionnez l'affectation de dispositif puis cliquez sur **Next**.
5. Si vous avez sélectionné un dispositif pour la haute disponibilité, indiquez si le dispositif est une console.
6. Pour le type de configuration, sélectionnez **Normal Setup (default)** ou **HA Recovery Setup** et paramétrez la durée.
7. Si vous avez sélectionné **HA Recovery Setup**, entrez l'adresse IP virtuelle du cluster.
8. Sélectionnez la version de protocole IP :
   - Sélectionnez **ipv4** ou **ipv6**.
9. Si vous avez sélectionné **ipv6**, sélectionnez **manual** ou **auto** pour l'option **Configuration type**.
10. Sélectionnez la configuration de l'interface liée, si nécessaire.
11. Sélectionnez l'interface de gestion.
12. Dans l'assistant, entrez un nom de domaine complet dans la zone **Hostname**.

13. Dans la zone **IP address**, 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*.
14. Si vous ne disposez pas d'un serveur de messagerie, entrez `localhost` dans la zone **Email server name**.
15. Entrez les mots de passe `root` et `admin` respectant les critères suivants :
    - Il doit contenir au moins 5 caractères.
    - Il ne doit pas contenir d'espaces.
    - Il peut comporter les caractères spéciaux suivants : @, #, ^ et *.
16. Cliquez sur **Finish**.
17. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.

    La procédure d'installation peut prendre plusieurs minutes.
18. 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 **Connexion à 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**.
19. 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 matériel

Pour garantir la réussite de l'installation d'IBM Security QRadar sur votre propre matériel, 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 matérielle du dispositif 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 13.

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 matériel

Avant d'installer le système d'exploitation Red Hat Enterprise Linux (RHEL) sur votre propre matériel de 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 3. Configuration système requise pour les installations RHEL sur votre propre dispositif

Conditions requises	Description
Version de logiciel prise en charge	V7.3
Version de bits	64 bits
Disques KickStart	Non 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'événements	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.

Important : Désactivez SELinux (Security-Enhanced Linux) et redémarrez votre dispositif avant de commencer à installer QRadar.

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 4. 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 le répertoire `/media/cdrom`
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. 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 `/store` et entraîne une perte de données.
4. 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 matériel

Si vous utilisez votre propre matériel de 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.

Le système de fichiers de chaque partition est XFS.

Tableau 5. Guide de partitionnement pour RHEL

Chemin de montage	LVM pris en charge ?	Existe dans l'installation logicielle ?	Taille
/boot	Non	Oui	1 Go
/boot/efi	Non	Oui	200 Mo
/recovery	Non	Non	8 Go
/var	Oui	Oui	5 Go
/var/log	Oui	Oui	15 Go
/var/log/audit	Oui	Oui	3 Go
/opt	Oui	Oui	10 Go
/home	Oui	Oui	1 Go
/storetmp	Oui	Oui	15 Go
/tmp	Oui	Oui	3 Go
permutation	N/A	Oui	Formule de permutation : Configurez la taille de la partition de permutation pour qu'elle corresponde à 75 % de la mémoire RAM, avec une valeur minimale de 12 Gio et une valeur maximale de 24 Gio.
/	Oui	Oui	Jusqu'à 15 Go
/store	Oui	Oui	80 % d'espace restant
/transient	Oui	Oui	20 % d'espace restant

Configuration des partitions de la console pour plusieurs déploiements de disque

Pour les configurations matérielles incluant plusieurs disques, configurez les partitions de QRadar:

Disque 1

amorce, échange, système d'exploitation, fichiers temporaires QRadar et fichiers journaux

Disques restants

- Utilisez les configurations de stockage par défaut des dispositifs QRadar comme guides pour déterminer quel type RAID à utiliser.
- Montage en tant que /store
- Stockage des données QRadar

Le tableau ci-dessous présente la configuration de stockage par défaut pour les dispositifs QRadar.

Tableau 6. Configuration de stockage par défaut pour les dispositifs QRadar

Rôle de l'hôte QRadar	Configuration de stockage
Collecteur de flux QRadar Network Insights (QNI)	RAID1
Noeud de données Processeur d'événements Processeur de flux Processeur d'événement et de flux Console tout-en-un	RAID6
Collecteur d'événements	RAID10

Installation de RHEL sur votre propre matériel

Vous pouvez installer le système d'exploitation Red Hat Enterprise Linux (RHEL) sur votre propre matériel de dispositif afin de 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 matériel», à la page 15.

Procédure

1. Copiez l'image ISO du DVD du système d'exploitation Red Hat Enterprise Linux V7.3 sur 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 effectuer l'installation, suivez les instructions de l'assistant d'installation :
   a. Sélectionnez votre langue.
   b. Cliquez sur **Date & Time** et définissez l'heure de votre déploiement.
   c. Cliquez sur **Installation Destination** puis sélectionnez l'option **I will configure partitioning**.
   d. Sélectionnez **LVM** dans la liste déroulante.

e. Cliquez sur le bouton **Add** pour ajouter les capacités et les points de montage de vos partitions, puis cliquez sur **Done**. Pour plus d'informations sur les partitions RHEL7, voir «Propriétés de la partition du système d'exploitation Linux pour les installations QRadar sur votre propre matériel», à la page 17.

f. Cliquez sur **Network & Host Name**.

g. Entrez le nom d'hôte de votre dispositif.

h. Sélectionnez l'interface dans la liste, placez le commutateur en position **ON** puis cliquez sur **Configure**.

i. Sur l'onglet **General**, sélectionnez l'option **Automatically connect to this network when it is available**.

j. Dans l'onglet **IPv4 Settings**, sélectionnez **Manual** dans la liste **Method**.

k. Cliquez sur **Add** pour entrer l'adresse IP, le masque de réseau et la passerelle du dispositif dans la zone **Addresses**.

l. Ajoutez deux serveurs DNS.

m. Cliquez sur **Save** > **Done** > **Begin Installation**.

6. Définissez le mot de passe root puis cliquez sur **Finish configuration**.
7. Redémarrez le dispositif à la fin de l'installation.

Référence associée:

«Propriétés de la partition du système d'exploitation Linux pour les installations QRadar sur votre propre matériel», à la page 17
Si vous utilisez votre propre matériel de 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.

Installation de QRadar après celle de RHEL

Installez IBM Security QRadar sur votre dispositif après avoir installé RHEL.

Avant de commencer

Dans de rares circonstances, il peut être nécessaire d'installer RHEL séparément de QRadar. Dans ce cas, vous devez installer Red Hat Enterprise Linux (RHEL) V7.3 sur le système sur lequel vous voulez installer QRadar. Pour plus d'informations, voir «Installation de RHEL sur votre propre matériel», à la page 19.

Procédure

1. En utilisant un programme SFTP, tel WinSCP, copiez l'élément ISO QRadar sur l'hôte où vous souhaitez installer QRadar.
2. Sur l'hôte sur lequel vous installez QRadar, créez un répertoire `/media/cdrom` avec la commande suivante :

   ```
   mkdir /media/cdrom
   ```

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

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

4. Exécutez la configuration QRadar en utilisant la commande suivante :

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

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.

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 inclut le logiciel QRadar installé sur un ordinateur virtuel.

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, vous devez les ajouter à votre déploiement. Pour plus d'informations sur la procédure de connexion des dispositifs virtuels après leur installation, voir *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 Event Collector Virtual 1599
- QRadar Data Node Virtual 1400
- QRadar QFlow Virtual 1299
- QRadar Event Collector Virtual 1599

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 Event Collector 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 1 000 objets réseau
- 1200000 flux par intervalle, en fonction de votre licence
- 30000 événements par seconde, en fonction de 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'événements 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 :

- 1200000 flux par intervalle, en fonction de votre licence
- 30000 événements par seconde, en fonction de votre licence
- Stockage de flux dédié de 2 To ou plus
- 1 000 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 un processeur de flux dédié que vous pouvez utiliser pour échelonner votre déploiement QRadar SIEM afin de gérer des taux de flux par intervalle plus élevés. QRadar SIEM Flow Processor Virtual 1799 comporte un processeur de flux intégré et un stockage interne pour les flux.

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

- 3600000 flux par intervalle, en fonction des types de trafic
- Stockage de flux dédié de 2 To ou plus
- 1 000 objets réseau
- Contrôle de l'activité réseau QRadar QFlow Collector et Layer 7

Le dispositif QRadar SIEM Flow Processor Virtual 1799 est un dispositif Processeur de flux réparti qui requiert une connexion à un dispositif QRadar SIEM série 31XX.

QRadar SIEM Event Processor Virtual 1699

Ce dispositif virtuel est un processeur d'événements 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 Event Collector dédié, un processeur d'événements et un stockage interne pour les événements.

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

- Jusqu'à 80000 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'événements réparti qui requiert une connexion à un dispositif QRadar SIEM série 31XX.

QRadar Event Collector Virtual 1599

Ce dispositif virtuel est un Event Collector 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 Event Collector Virtual 1599 inclut un Event Collector dédié, un processeur d'événements et un stockage interne pour les événements.

Le dispositif QRadar Event Collector Virtual 1599 prend en charge les éléments suivants :

- Jusqu'à 20000 événements par seconde
-

Le dispositif virtuel QRadar Event Collector Virtual 1599 est un dispositif Event Collector réparti qui requiert une connexion à un dispositif QRadar SIEM série 31XX.

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 en utilisant le type de dispositif Noeud de données 1400.

QRadar QFlow Virtual 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 QFlow Virtual 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 QFlow Virtual 1299 ne prend pas en charge NetFlow.

Configuration système requise pour les dispositifs virtuels

Pour vérifier que IBM Security QRadar fonctionne correctement, vous devez utiliser des dispositifs virtuels dotés de la configuration minimale.

Le dispositif virtuel doit avoir au moins 256 Go de stockage disponible. Avant d'installer votre dispositif virtuel, utilisez la formule suivante pour déterminer vos besoins en matière de stockage :

(nombre de jours) x (secondes dans une journée) x (débit d'événements par seconde) x (taille moyenne d'un événement de consignation x 1,5 temps système d'événement normalisé QRadar) x 1,05 / (1000 x 1000 x 1000) + 40 Go

Exemple : 30 x 86400 x 1000 EPS x 600 octets x 1,05 / (1000 x 1000 x 1000) + 40 Go = 1673 Go

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

Tableau 7. Quantité de mémoire minimale et suggérée pour les dispositifs virtuels QRadar

Dispositif	Mémoire requise minimale	Mémoire requise recommandée
QRadar QFlow Virtual 1299	6 Go	6 Go
Dispositif QRadar Data Node Virtual 1400	12 Go	48 Go
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 8099	24 Go	48 Go
QRadar Risk Manager	24 Go	48 Go
QRadar Vulnerability Manager Processeur	32 Go	32 Go
Scanner QRadar Vulnerability Manager	16 Go	16 Go

Le tableau ci-dessous indique la quantité de mémoire minimale requise pour les dispositifs virtuels.

Tableau 8. Unité centrale requise pour les dispositifs virtuels QRadar

Application QRadar	Seuil	Nombre minimal de coeurs d'UC	Nombre de coeurs d'UC suggéré
QRadar Log Manager Virtual 8099	2500 événements par seconde (EPS) ou moins	4	16
	5000 EPS ou moins	8	16
QRadar Event Collector Virtual 1599	2500 EPS ou moins	4	16
	5000 EPS ou moins	8	16
	20000 EPS ou moins	16	16
QRadar SIEM Event Processor Virtual 1699	2500 EPS ou moins	4	24
	5000 EPS ou moins	8	24
	20000 EPS ou moins	16	24

Tableau 8. Unité centrale requise pour les dispositifs virtuels QRadar (suite)

Application QRadar	Seuil	Nombre minimal de coeurs d'UC	Nombre de coeurs d'UC suggéré
QRadar SIEM All-in-One Virtual 3199	25000 flux par minute (FPM) ou moins 500 EPS ou moins	4	24
	50000 FPM ou moins 1000 EPS ou moins	8	24
	100000 FPM ou moins 1000 EPS ou moins	12	24
	200000 FPM ou moins 5000 EPS ou moins	16	24
QRadar SIEM Flow Processor Virtual 1799	150000 FPM ou moins	4	24
	300000 FPM ou moins	8	24
QRadar QFlow Virtual 1299	10000 FPM ou moins	4	4
QRadar Vulnerability Manager Processeur		4	4
Scanner QRadar Vulnerability Manager		4	4
QRadar Risk Manager		8	8
Dispositif QRadar Data Node Virtual 1400		4	16

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 9. 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

Tableau 9. Configuration minimale requise pour les dispositifs lors d'une installation virtuelle ou logicielle. (suite)

Classification système	Informations sur le dispositif	IOPS	Vitesse de transfert des données (Mo/s)
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 ESXi pour créer un ordinateur virtuel.

Création de votre ordinateur virtuel

Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESXi 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 **Virtual Machine Version**, sélectionnez une version matérielle de machine virtuelle prise en charge par la version de VMWare ESXi que vous utilisez. Utilisez le tableau suivant pour sélectionner une version prise en charge.

Tableau 10. Versions matérielles de machine virtuelle prises en charge

VMWare ESXi version	Versions matérielles de machine virtuelle
VMWare ESXi 6.0	Versions 7 à 11
VMWare ESXi 5.5	Versions 7 à 10
VMWare ESXi 5.1	Versions 7 à 9
VMWare ESXi 5.0	Versions 7 et 8

Pour plus d'informations, voir ESXi/ESX hosts and compatible virtual machine hardware versions list (https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2007240).

   c. Pour le **système d'exploitation**, sélectionnez **Linux** et **Red Hat Enterprise Linux 7 (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 11. Descriptions des paramètres de configuration réseau

Paramètre	Description
Nombre de NIC à connecter	Vous devez ajouter au moins une carte d'interface réseau.
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 12. 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.

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 **Summary**.
3. Dans le volet **Commands**, cliquez sur **Edit Setting**.
4. Dans le volet de gauche de la fenêtre **Virtual Machine Properties**, cliquez sur **CD/DVD Drive 1**.
5. Dans le panneau **Device Type**, sélectionnez **DataStore ISO File**.
6. Dans le volet **Device Status**, cochez la case **Connect at power on**.
7. Dans le panneau **Device Type**, cliquez sur **Browse**.
8. Dans la fenêtre Browse Datastores, recherchez et sélectionnez le fichier ISO du produit QRadar, cliquez sur **Open**, 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 **Power** > **Power On**.
10. Connectez-vous à l'ordinateur virtuel en entrant `root` comme nom d'utilisateur.

    Le nom d'utilisateur dépend des minuscules/majuscules.
11. Acceptez le contrat de licence utilisateur final.
12. Sélectionnez le type de dispositif :
    - **Non-Software Appliance**
    - **Software Appliance**
13. Sélectionnez l'affectation de dispositif puis sélectionnez **Next**.
14. Si vous avez sélectionné un dispositif pour la haute disponibilité, indiquez si le dispositif est une console.
15. Pour le type de configuration, sélectionnez **Normal Setup (default)** ou **HA Recovery Setup** et paramétrez la durée.
16. Si vous avez sélectionné **HA Recovery Setup**, entrez l'adresse IP virtuelle du cluster.
17. Sélectionnez la version de protocole IP :
    - Sélectionnez **ipv4** ou **ipv6**.
18. Si vous avez sélectionné **ipv6**, sélectionnez **manual** ou **auto** pour l'option **Configuration type**.
19. Sélectionnez la configuration de l'interface liée, si nécessaire.
20. Sélectionnez l'interface de gestion.
21. Dans l'assistant, entrez un nom de domaine complet dans la zone **Hostname**.
22. Dans la zone **IP address**, 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*.
23. Si vous ne disposez pas d'un serveur de messagerie, entrez `localhost` dans la zone **Nom du serveur de messagerie**.
24. Entrez les mots de passe `root` et `admin` respectant les critères suivants :
    - Il doit contenir au moins 5 caractères.
    - Il ne doit pas contenir d'espaces.
    - Il peut comporter les caractères spéciaux suivants : @, #, ^ et *.
25. Cliquez sur **Finish**.
26. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.

    La procédure d'installation peut prendre plusieurs minutes.
27. 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 **Connexion à 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 27
Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESXi pour créer un ordinateur virtuel.

Ajout de votre 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 **Connexion à 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 27
Pour installer un dispositif virtuel, vous devez d'abord utiliser VMWare ESXi pour créer un ordinateur virtuel.

Chapitre 6. Installations 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.

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

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 **Connexion à 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 de l'élément ISO QRadar pour l'édition à installer.
- Vous devez installer Red Hat Enterprise Linux (RHEL) V7.3 sur le système où vous souhaitez installer QRadar. Pour plus d'informations, voir «Installation de RHEL sur votre propre matériel», à la page 19.
- Modifiez la valeur SELINUX dans le fichier `/etc/sysconfig/selinux` en `SELINUX=disabled` et redémarrez le système.

Procédure

1. En tant que superutilisateur, utilisez SSH pour vous connecter à l'hôte sur lequel installer QRadar.
2. Dans le répertoire racine de l'hôte où vous souhaitez installer QRadar, créez un fichier nommé `AUTO_INSTALL_INSTRUCTIONS` contenant les éléments suivants :

Tableau 13. Paramètres du fichier d'installation silencieuse. Les paramètres répertoriés comme facultatifs sont requis dans le fichier `AUTO_INSTALL_INSTRUCTIONS` mais ils peuvent n'inclure aucune valeur.

Paramètre	Valeur requise ?	Description	Valeurs autorisées
`force`	Obligatoire	Provoque l'installation du dispositif malgré des problèmes matériels.	`true` ou `false`
`api_auth_token`	Facultatif	Jeton d'autorisation. Pour plus d'informations sur la gestion des services autorisés, voir le document *IBM Security QRadar Administration Guide*.	Jeton d'autorisation
`appliance_number`	Facultatif	Identificateur du dispositif	`0`, `3105`, `1201`, et ainsi de suite.
`appliance_oem`	Obligatoire	Identifie le fournisseur du dispositif.	`qradar`, `forensics`, etc.
`appliance_filter`	Obligatoire	Nom ou identificateur du dispositif.	`vmware`, `na`
`bonding enabled`	Obligatoire.	Indique si vous utilisez des interfaces liées.	`true` ou `false`
`bonding _interface`	Obligatoire si des interfaces liées sont utilisées.	Adresses MAC des interfaces que vous liez, séparées par des virgules.	*<nom_interface =adresse_mac>, <nom_interface_esclave =adresse_mac>*

Tableau 13. Paramètres du fichier d'installation silencieuse (suite). Les paramètres répertoriés comme facultatifs sont requis dans le fichier `AUTO_INSTALL_INSTRUCTIONS` mais ils peuvent n'inclure aucune valeur.

Paramètre	Valeur requise ?	Description	Valeurs autorisées
`bonding_interface_name`	Obligatoire si des interfaces liées sont utilisées.	Identifie l'interface de liaison.	`bond0`
`bonding_options`	Obligatoire si des interfaces liées sont utilisées.	Options Linux pour les interfaces liées. Pour plus d'informations sur la liaison de carte d'interface réseau, voir le document *IBM Security QRadar Administration Guide*.	**Exemple :** `miimon=100 mode=4 lacp_rate=1`
`email_server`	Obligatoire	Serveur de messagerie ou nom SMTP, tel `localhost.`	
`ha_cluster_virtual_ip`	Facultatif	Indique l'adresse IP du cluster HA.	`ip_address`
`hostname`	Obligatoire	Nom d'hôte complet de votre système QRadar.	
`ip_protocol`	Obligatoire	Protocole IP pour cet hôte.	`ipv4`, `ipv6`
`ip_dns_primary`	Si la valeur `IPv4` est indiquée pour `ip_protocol`, cet élément est requis	Serveur DNS principal.	Adresse IPv4 valide.
`ip_dns_secondary`	Si la valeur `IPv4` est indiquée pour `ip_protocol`, cet élément est requis	Serveur DNS secondaire.	Adresse IPv4 valide.
`ip_management_interface`	Obligatoire	Nom d'interface et adresse MAC de l'interface de gestion. Vous pouvez utiliser l'une ou l'autre de ces informations, ou les deux, séparées par "=".	
`ipv4_address`	Si la valeur `IPv4` est indiquée pour `ip_protocol`, cet élément est requis	Adresse IP de l'hôte sur lequel vous installez le logiciel.	Adresse IPv4 valide

Tableau 13. Paramètres du fichier d'installation silencieuse (suite). Les paramètres répertoriés comme facultatifs sont requis dans le fichier `AUTO_INSTALL_INSTRUCTIONS` mais ils peuvent n'inclure aucune valeur.

Paramètre	Valeur requise ?	Description	Valeurs autorisées
`ipv4_address _public`	Si `ip_protocol` a la valeur `IPv4` et qu'il existe des conversions d'adresses réseau, cet élément est requis	Adresse IP publique de l'hôte sur lequel vous installez le logiciel.	Adresse IPv4 valide
`ipv4_gateway`	Si la valeur `IPv4` est indiquée pour `ip_protocol`, cet élément est requis	Passerelle réseau de cet hôte	Adresse IPv4 valide
`ipv4_nework_mask`	Si la valeur `IPv4` est indiquée pour `ip_protocol`, cet élément est requis	Masque de réseau de cet hôte	
`ip_v6_address`	Si `ip_protocol` a la valeur `IPv6`, cet élément est requis	Adresse IPv6 de l'installation QRadar, si nécessaire.	Adresse IPv6 valide
`ip_v6_address _public`	Si `ip_protocol` a la valeur `IPv6` et qu'il existe des conversions d'adresses réseau, cet élément est requis	Adresse IP publique de l'hôte sur lequel vous installez le logiciel.	Adresse IPv6 valide
`ip_v6_autoconf`	Obligatoire	Indique si IPv6 est configuré automatiquement.	`true` ou `false`
`ip_v6_gateway`	Non requis	N'indiquez aucune valeur pour ce paramètre.	

Tableau 13. Paramètres du fichier d'installation silencieuse (suite). Les paramètres répertoriés comme facultatifs sont requis dans le fichier `AUTO_INSTALL_INSTRUCTIONS` mais ils peuvent n'inclure aucune valeur.

Paramètre	Valeur requise ?	Description	Valeurs autorisées
`is_console`	Obligatoire	Indique si cet hôte correspond à la console lors du déploiement	`true` - Cet hôte correspond à la console lors du déploiement `false` - Cet hôte ne correspond pas à la console mais à un autre type d'hôte géré (processeur d'événements ou de flux, etc.)

`is_console`
 	
`_standby`
	Obligatoire.	Indique si cet hôte est une console à haute disponibilité de secours	`true` ou `false`

`admin_password`	Facultatif.	Mot de passe du compte administrateur. Vous pouvez chiffrer le mot de passe, si nécessaire. Si vous ne renseignez pas ce paramètre, le mot de passe n'est pas mis à jour.	*<password>* **Important :** Les politiques de sécurité de votre entreprise peuvent vous empêcher d'entrer un mot de passe dans un fichier statique du dispositif. `Defined` ou n'indiquez aucune valeur pour utiliser un mot de passe précédemment entré lors d'une mise à niveau.
`root_password`	Obligatoire	Mot de passe du compte root. Vous pouvez chiffrer le mot de passe, si nécessaire. Si vous ne renseignez pas ce paramètre, le mot de passe n'est pas mis à jour.	*<password>* **Important :** Les politiques de sécurité de votre entreprise peuvent vous empêcher d'entrer un mot de passe dans un fichier statique du dispositif. `Defined` ou n'indiquez aucune valeur pour utiliser un mot de passe précédemment entré lors d'une mise à niveau.

`security`
 	
`_template`
	Si `isconsole` est défini sur `Y`, puis obligatoire	Modèle de sécurité
		
		Cette valeur doit être cohérente avec celle entrée dans `appliance_number`.
			`Enterprise` - pour tous les hôtes basés sur SIEM
			
			`Logger` - pour le gestionnaire de journaux

Tableau 13. Paramètres du fichier d'installation silencieuse (suite). Les paramètres répertoriés comme facultatifs sont requis dans le fichier `AUTO_INSTALL_INSTRUCTIONS` mais ils peuvent n'inclure aucune valeur.

Paramètre	Valeur requise ?	Description	Valeurs autorisées
`time_current_date`	Obligatoire	Date courante de cet hôte. Utilisez le format suivant : `YYYY/MM/DD`	
`time_current_time`	Obligatoire	Heure de l'hôte au format 24 heures `HH:MM:SS`.	
`time_ntp_server`	Facultatif	FQHN ou adresse IP du serveur NTP (Network Time Protocol).	

`timezone`	Obligatoire	Fuseau horaire de la base de données TZ. Pour plus d'informations, voir http://timezonedb.com/.	`Europe/London`
			`GMT`
			`America/Montreal`
			`America/New_York`
			`America/Los_Angeles`
			`Asia/Tokyo`, etc.

`type_of_setup`	Obligatoire	Indique le type d'installation pour cet hôte.	`normal`- Déploiement d'hôte géré ou de console QRadar standard. `recovery` - Installation de récupération à haute disponibilité (HA) sur cet hôte.
`console_host`	Requis pour SIOC	Nom de votre système IBM QRadar on Cloud.	Adresse IP
`Gateway setup choice`	Requis pour SIOC	Entrez `True` si ce disponible se trouve dans une passerelle IBM QRadar on Cloud. Entrez `False` si le dispositif ne se trouve pas dans un dispositif de passerelle.	`true` ou `false`
`http_proxy_host`	Facultatif	Nom d'hôte de l'hôte proxy pour le dispositif IBM QRadar on Cloud.	
`http_proxy_password`	Facultatif	Mot de passe de l'hôte proxy pour le dispositif IBM QRadar on Cloud.	
`http_proxy_port`	Facultatif	Identificateur du port de connexion sur l'hôte proxy pour le dispositif IBM QRadar on Cloud.	
`http_proxy_user`	Facultatif	Nom d'utilisateur de l'hôte proxy pour le dispositif IBM QRadar on Cloud.	

Tableau 13. Paramètres du fichier d'installation silencieuse (suite). Les paramètres répertoriés comme facultatifs sont requis dans le fichier AUTO_INSTALL_INSTRUCTIONS mais ils peuvent n'inclure aucune valeur.

Paramètre	Valeur requise ?	Description	Valeurs autorisées
internet_access _mode	Requis pour SIOC	Mode à utiliser pour l'accès au dispositif IBM QRadar on Cloud	direct ou proxy

Exemple :

```
#0.0.1
ai_force=<true_ou_false>
ai_api_auth_token= <certificat>
ai_appliance_number= <####>
ai_appliance_oem= <qradar_forensics_ou_oem>
ai_appliance_filter= <ID_ou_numéro_dispositif>
ai_bonding_enabled= <true_ou_false>
ai_bonding_interfaces= <adresse_mac>
ai_bonding_interface_name= <ID_interface>
ai_bonding_options= <ID_option_de_liaison>
ai_email_server= <nom_smtp>
ai_gateway_setup_choice= <true_ou_false>
ai_ha_cluster_virtual_ip= <adresse_IP>
ai_hostname= <nom_hôte_avec_FQDN>
ai_ip_dns_primary= <adresse_IP_DNS_principal>
ai_ip_dns_secondary= <adresse_IP_DNS_secondaire>
ai_ip_management_interface= <adresse_MAC>
ai_ip_protocol= <ipv4_ou_ipv6>
ai_ip_v4_address= <adresse_IP>
ai_ip_v4_address_public= <adresse_IP_publique>
ai_ip_v4_gateway= <adresse_IP_passerelle>
ai_ip_v4_network_mask= <masque_réseau>
ai_ip_v6_address= <adresse_IPv6>
ai_ip_v6_address_public= <adresse_IPv6_publique>
ai_ip_v6_autoconf= <true_ou_false>
ai_ip_v6_gateway= <adresse_IP>
ai_is_console= <true_ou_false>
ai_is_console_standby= <true_ou_false>
ai_root_password= <mot_de_passe_compte_root>
ai_security_template= <enterprise_ou_logger>
ai_time_current_date= <aaaa-mm-jj>
ai_time_current_time= <hh:mm:ss>
ai_time_ntp_server= <serveurNtp_serveurHôte>
ai_timezone= <EST_ou_PST_ou_fuseau_horaire>
ai_type_of_setup= <normal_ou_recovery>
ai_console_host= <adresse_IP_ou_ID_hôte_SIOC_7000>
ai_http_proxy_host= <nom_hôte_proxy_SIOC_7000>
ai_http_proxy_password= <mot_de_passe_proxy_SIOC_7000>
ai_http_proxy_port= <port_proxy_SIOC_7000>
ai_http_proxy_user= <nom_utilisateur_proxy_SIOC_7000>
ai_internet_access_mode= <SIOC_7000_direct_ou_proxy>
```

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.

3. En utilisant un programme SFTP, tel WinSCP, copiez l'élément ISO QRadar sur l'hôte où vous souhaitez installer QRadar.

4. Sur l'hôte où vous effectuez l'installation, créez un répertoire `/media/cdrom` en utilisant la commande suivante :

   ```
   mkdir /media/cdrom
   ```

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

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

6. Exécutez la configuration QRadar en utilisant la commande suivante :

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

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

Vous pouvez installer des instances du logiciel IBM Security QRadar sur un serveur cloud 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), 10000 (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 Services

Configurez IBM Security QRadar dans une instance AWS (Amazon Web Services).

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-7.3_HVM_GA-20161026-x86_64-1-Hourly2-GP2`, disponible dans les **éléments AMI de communauté**
Type d'instance	Sélectionnez une instance qui dispose de la configuration système requise pour les dispositifs virtuels

Tableau 14. Instance AWS requise (suite)

Conditions requises	Valeur
Stockage	Deux disques : 1 volume de 100 Go Un volume pour le stockage, basé sur la formule suivante (minimum 100 Go) : (nombre de jours) x (secondes dans une journée) x (débit d'événements par seconde) x (taille moyenne d'un événement de consignation x 1,5 temps système d'événement normalisé QRadar) x 1,05 / (1000 x 1000 x 1000) + 40 Go **Exemple :** 30 x 86400 x 1000 EPS x 600 octets x 1,05 / (1000 x 1000 x 1000) + 40 Go = 1673 Go
Groupe de sécurité	Adresses IP de la liste, avec les ports 22 et 443 ouverts.

3. Téléchargez le script AWS QRadar Install Helper depuis Fix Central (www.ibm.com/support/fixcentral/).
   a. Accédez à l'onglet **Sélectionner un produit**.
   b. Dans **Groupe de produits**, sélectionnez **IBM Security**.
   c. Dans **Sélection dans IBM Security**, choisissez **IBM Security QRadar SIEM**.
   d. Dans **Version installée**, sélectionnez **7.3.0** et cliquez sur **Continuer**.
   e. Sélectionnez **Recherchez des correctifs** et cliquez sur **Continuer**.
   f. Cliquez sur **SCRIPT**.
   g. Sélectionnez le script AWS QRadar Install Helper.

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

Pourquoi et quand exécuter cette tâche

Tenez compte des éléments suivants lorsque vous exécutez la procédure :

- La configuration haute disponibilité n'est pas prise en charge dans les installations QRadar AWS.
- Les valeurs des commandes utilisées dans la procédure ne sont que des exemples. Elles peuvent varier d'un déploiement à un autre.

Avertissement :

- N'exécutez pas la commande **`yum update`** avant ou après l'installation. La mise à niveau de l'installation QRadar met à jour les packages du système d'exploitation.
- Ne créez pas de partitions et n'effectuez pas d'opérations de gestion LVM avant d'avoir exécuté le script AWS QRadar Install Helper. Ce script configure les partitions nécessaires. Vous pouvez augmenter la taille des volumes LVM configurés après l'exécution du script ou l'installation de QRadar.

Procédure

1. Pour copier le script qui prépare les partitions et les options de configuration AWS dans l'instance AWS, tapez la commande suivante :

```
scp -i <key.pem> aws_qradar_prep.sh ec2-user@<adresse_IP_publique>:
```

2. 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 <key.pem> ec2-user@<adresse_IP_publique>
   ```

3. Pour exécuter le script qui prépare les partitions et les options de configuration AWS, tapez la commande suivante :

   ```
   sudo bash +x ./aws_qradar_prep.sh --install
   ```

   L'instance AWS redémarre à l'issue de l'exécution du script.

4. Pour copier l'image ISO sur le périphérique, entrez la commande suivante :

   ```
   scp -i <key.pem> <qradar.iso> ec2-user@<adresse_IP_publique>:
   ```

5. Pour monter l'image ISO, entrez les commandes suivantes :

   ```
   sudo mount -o loop /home/ec2-user/<qradar.iso> /media/cdrom
   ```

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

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

7. Entrez `Y` lorsque vous êtes invité à accepter une installation sur un matériel non pris en charge.
8. Suivez les invites pour exécuter l'assistant d'installation de QRadar.

   Important : Vous devez indiquer un mot de passe root à l'invite du programme.

Configuration des noeuds finaux de serveur pour les installations de 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_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 avoir 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 de 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 s'appellent `<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 de 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. 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** window.

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.

Important : Dans les éditions précédentes de QRadar, les interfaces étaient nommées en utilisant le format suivant : `eth0`, `eth1`, `eth4`, etc. L'éventail de noms possibles pour l'interface QRadar version 7.3.0 est plus étendu. Par exemple, `ens192`, `enp2s0`, etc.

Votre fichier de paramètres réseau peut se présenter comme dans l'exemple ci-dessous, où *NAME="<old_name>"* correspond à la carte d'interface réseau remplacée et *NAME="<new_name>"* correspond à la carte d'interface réseau installée.

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

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

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

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

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 les deux lignes correspondant au remplacement de la carte d'interface réseau : `NAME="<old_name>"`.
5. Renommez les valeurs `Name=<name>` de la carte d'interface réseau nouvellement installée.

   Exemple : Renommez `NAME="<new_name>"` en `NAME="<old_name>"`.
6. Enregistrez le fichier et fermez-le.
7. Entrez la commande suivante : `reboot`.

Chapitre 10. 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.

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 55
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 54
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'événements 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		Le module 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 Event Collector et le composant local processeur d'événements 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 66.
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 Event Collector vers QRadar Console.	Diffusion en temps réel (diffusion en flux) des événements.
7801	Apache Tomcat	TCP	Depuis le Event Collector vers QRadar Console.	Diffusion en temps réel (diffusion en flux) des flux.
7803	Apache Tomcat	TCP	Depuis le Event Collector 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 Event Collector 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 Collectors
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 allouent 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 d'IMQ en utilisant Telnet pour vous connecter à l'hôte local et en effectuant une recherche sur le numéro de port.

Le associations de port aléatoires ne sont pas des numéros de port statiques. Lorsqu'un service redémarre, les ports générés pour un service sont réalloués 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 similaires à la sortie suivante :

   ```
   [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=<session_id>]
   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 telnet présente 3 des 4 ports TCP à valeur aléatoire élevée pour IMQ. Le quatrième port, qui n'est pas affiché, est un port RMI JMX (Remote Method Invocation) disponible via l'URL JMX présentée dans la sortie.

   Si la connexion telnet est refusée, cela signifie qu'IMQ n'est pas actuellement en cours d'exécution. Il est possible que le système soit en cours de démarrage ou d'arrêt ou que les services aient été arrêtés 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	Serveurs de mise à jour automatique QRadar. 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).
qmmunity-eu.q1labs.com	Serveurs de mise à jour automatique QRadar. 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
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).