IBM Security QRadar Incident Forensics
Version 7.2.6

Guide d'installation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 35.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.6 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Présentation de l'installation d'IBM Security QRadar Incident Forensics

Le présent document fournit des informations sur l'installation d'IBM® Security QRadar Incident Forensics et l'intégration du produit à IBM Security QRadar. Les dispositifs QRadar Incident Forensics comportent des logiciels préinstallés et le système d'exploitation Red Hat Enterprise Linux. Vous pouvez également installer le logiciel QRadar Incident Forensics sur votre matériel.

Utilisateurs concernés

Administrateurs réseau chargés de l'installation et de la configuration des systèmes QRadar Incident Forensics.

Administrateurs nécessitant des connaissances sur l'exploitation des réseaux et les systèmes d'exploitation Linux.

Documentation technique

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

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

Contacter le service clients

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

Déclaration de pratiques de sécurité recommandées

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

Remarque/Commentaire :

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

Important

IBM Security QRadar Incident Forensics est conçu pour aider les sociétés à améliorer leur environnement et leurs données de sécurité. Plus spécifiquement, IBM Security QRadar Incident Forensics est conçu pour aider les sociétés à examiner et à mieux comprendre ce qui s'est passé lors d'incidents de sécurité réseau. L'outil permet aux sociétés d'indexer et de rechercher des données de paquets réseau capturés (PCAP) et inclut une fonction permettant de reconstruire ces données à leur forme initiale. Cette fonction de reconstruction peut reconstruire des données et des fichiers, y compris des messages électroniques, des fichiers et des images joints, des appels téléphoniques voix sur IP (VoIP) et des sites Web. Pour plus d'informations sur les caractéristiques et les fonctions du programme et la façon dont elles peuvent être configurées, consultez les manuels et les autres documents accompagnant le programme. L'utilisation de ce programme peut impliquer différentes lois et réglementations, dont celles concernant la confidentialité, la protection des données, l'emploi, les communications électroniques et le stockage. IBM Security QRadar Incident Forensics peut être utilisé à des fins légales, dans le respect de la loi. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le détenteur de la licence admet qu'il a obtenu ou va obtenir l'acceptation, l'autorisation ou la licence lui permettant de faire un usage légal d'IBM Security QRadar Incident Forensics.

Chapitre 1. Mise à niveau de QRadar Incident Forensics

Vous devez mettre à niveau tous vos produits IBM Security QRadar de votre déploiement vers la même version. Mettez à niveau IBM Security QRadar Incident Forensics version 7.2.5 vers version 7.2.6 à l'aide d'un programme d'installation de mise à niveau. Cette opération permet de mettre à niveau RedHat Enterprise Linux vers la version 6.7.

Si vous souhaitez effectuer une mise à niveau depuis QRadar Incident Forensics version 7.2.4 ou des versions antérieures et conserver vos données, contactez votre ingénieur commercial IBM. Sinon, si vous souhaitez effectuer une mise à niveau depuis QRadar Incident Forensics version 7.2.4 ou des versions antérieures mais que vous ne souhaitez pas conserver vos données, mettez à niveau directement vers version 7.2.6 en effectuant une nouvelle installation.

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

Procédure

1. Téléchargez le fichier <*QRadar_patchupdate*>.*sfs* depuis IBM Fix Central (www.ibm.com/support/fixcentral).
2. Utilisez SSH pour vous connecter à votre système comme utilisateur root.
3. Copiez le fichier correctif dans le répertoire `/tmp` ou tout autre emplacement disposant de suffisamment d'espace disque.
4. Pour créer le répertoire `/media/updates`, tapez la commande suivante :

   ```
   mkdir -p /media/updates
   ```
5. Accédez au répertoire dans lequel vous aviez le fichier correctif.
6. Pour monter le fichier correctif dans le répertoire `/media/updates`, tapez la commande suivante :

   ```
   mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
   ```
7. Pour exécuter le programme d'installation de mise à niveau, entrez la commande suivante :

   ```
   /media/updates/installer
   ```

   La première fois que vous exécutez le script du programme d'installation des correctifs, il peut y avoir un délai avant que le menu du programme d'installation du premier correctif s'affiche.
8. Répondez aux questions préalables à l'installation en fonction de votre déploiement.
9. Utilisez le programme de mise à niveau pour mettre à niveau tous les hôtes de votre déploiement.

   Si vous ne sélectionnez pas **Appliquer tous les correctifs**, vous devez mettre à niveau les systèmes dans l'ordre suivant :

   - QRadar Console
   - QRadar Incident Forensics

   Si votre session SSH est déconnectée alors que la mise à niveau est en cours, la mise à niveau continue. Lorsque vous rouvrez votre session SSH et que vous réexécutez le programme d'installation, l'installation reprend.

10. Une fois la mise à niveau effectuée, désinstallez la mise à jour logicielle à l'aide de la commande suivante : **umount /media/updates**

Que faire ensuite

Mettez à niveau vos périphériques de capture de paquet. Pour plus d'informations, voir *IBM Security QRadar Packet Capture Quick Reference Guide*.

Chapitre 2. Composants d'installation de QRadar Incident Forensics

QRadar Incident Forensics est intégré à l'architecture évolutive d'IBM QRadar Security Intelligence Platform. En fonction de vos besoins, vous pouvez installer des composants IBM Security QRadar Incident Forensics sur un seul dispositif (*tout-en-un*) ou sur plusieurs dispositifs.

Options d'installation

Les fonctions de sécurité disponibles varient selon les composants que vous installez. Par exemple, si vous installez QRadar Incident Forensics sur un seul dispositif, seules les fonctions réseau Forensics sont disponibles. En revanche, si vous installez un hôte géré QRadar Incident Forensics, vous disposez de fonctions de sécurité supplémentaires. Pour la plupart des installations, vous installez QRadar Console, au moins un composant QRadar Incident Forensics Processor et un ou plusieurs dispositifs QRadar Packet Capture.

Le diagramme ci-après récapitule les différentes fonctions de sécurité et les éléments de l'architecture d'IBM QRadar Security Intelligence Platform.

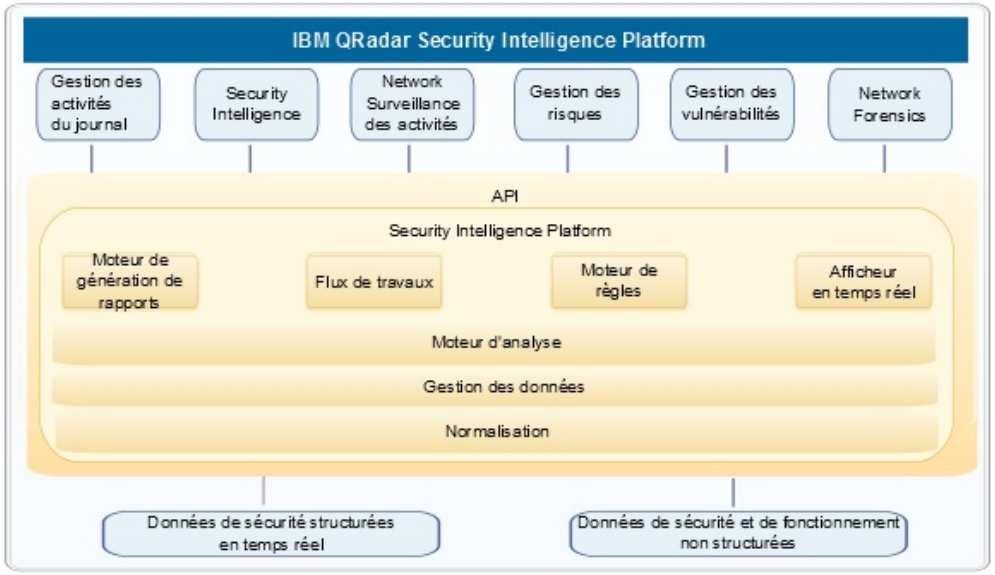


Figure 1. Présentation de l'architecture de la sécurité intelligente QRadar

Déploiements tout-en-un

Lors d'un déploiement autonome ou tout-en-un, vous installez le logiciel IBM Security QRadar Incident Forensics Standalone. Ces déploiements reviennent à installer le composant QRadar Console et l'hôte géré QRadar Incident Forensics sur un même dispositif sans les fonctions de gestion du journal, de surveillance de l'activité réseau ou d'autres fonctions de sécurité intelligente. Pour disposer d'une solution réseau Forensics autonome, installez QRadar Incident Forensics Standalone lors de déploiements de taille réduite et moyenne.

Comme indiqué dans le diagramme ci-après, vous pouvez connecter des dispositifs QRadar Packet Capture à IBM Security QRadar Incident Forensics Standalone.

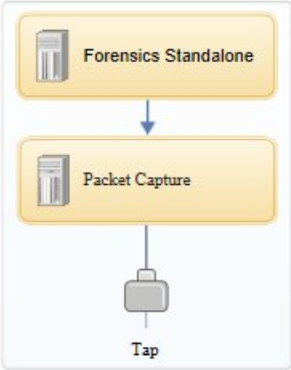


Figure 2. Exemple de déploiement d'IBM Security QRadar Incident Forensics Standalone

Restriction : Vous ne pouvez pas ajouter des hôtes gérés à QRadar Incident Forensics Standalone ni connecter QRadar Incident Forensics Standalone à QRadar Console.

Déploiements distribués

Si vous souhaitez effectuer des déploiements nécessitant une analyse réseau Forensics et d'autres fonctions de sécurité intelligente ou que vous devez distribuer la charge de travail pour des reprises Forensics, vous installez QRadar Console et un ou plusieurs hôtes gérés QRadar Incident Forensics. QRadar Console fournit des fonctions SIEM (Security Information and Event Management), des fonctions de gestion du journal, de détection des anomalies, de gestion des risques et de gestion des vulnérabilités.

Lors d'un déploiement distribué, il y a trois dispositifs :

- QRadar Console
- Hôte géré QRadar Incident Forensics (QRadar Incident Forensics Processor)
- QRadar Packet Capture (facultatif)

Lors d'un déploiement, tous les dispositifs IBM Security QRadar doivent posséder un niveau de version et de correctif identique. Les déploiements qui utilisent des versions de logiciel différentes ne sont pas pris en charge.

Le diagramme ci-après indique que vous pouvez connecter plusieurs hôtes gérés QRadar Incident Forensics au composant QRadar Console. Vous pouvez connecter des dispositifs QRadar Packet Capture aux hôtes gérés QRadar Incident Forensics (QRadar Incident Forensics Processor).

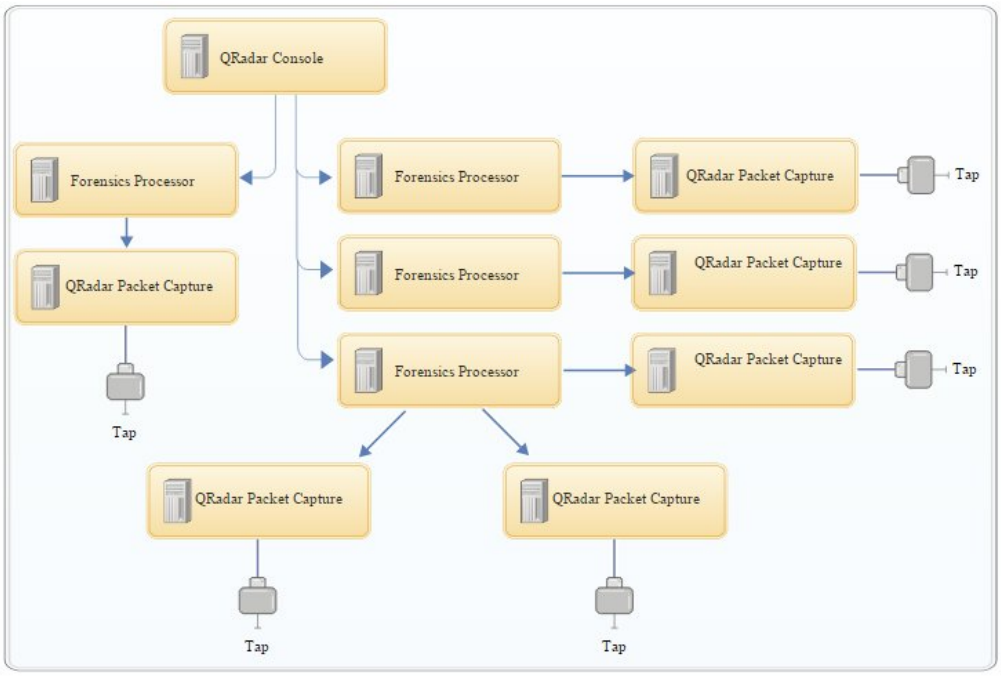


Figure 3. Exemple de déploiement distribué

Composants QRadar Incident Forensics

Les déploiements QRadar peuvent inclure les composants suivants :

QRadar Console

Fournit l'interface utilisateur du produit QRadar. Cette interface inclut des vues présentant les événements et les flux en temps réel, des rapports, des infractions, des informations sur les actifs et des fonctions d'adminstration.

Lors de déploiements distribués, utilisez QRadar Console pour gérer plusieurs hôtes QRadar Incident Forensics Processor.

QRadar Incident Forensics Processor

Fournit l'interface utilisateur du produit QRadar Incident Forensics. Cette interface contient des outils permettant de retracer les actions étape par étape des cybercriminels, de reconstituer les données réseau brutes liées à un incident de sécurité, d'effectuer des recherches dans des données non structurées et de reproduire visuellement les sessions et les événements.

Vous devez ajouter QRadar Incident Forensics Processor en tant qu'hôte géré pour pouvoir utiliser les fonctions Forensics de sécurité intelligente.

QRadar Incident Forensics Standalone

Fournit l'interface utilisateur du produit QRadar Incident Forensics. L'installation de QRadar Incident Forensics Standalone fournit les outils dont vous avez besoin pour effectuer des études Forensics. Seules les fonctions d'étude et d'administration Forensics associées sont disponibles.

QRadar Packet Capture

Vous pouvez installer un dispositif QRadar Packet Capture facultatif. S'il n'y a pas d'autre dispositif de capture de paquet réseau (PCAP) déployé, vous pouvez utiliser ce dispositif pour stocker les données utilisées par QRadar Incident Forensics. Vous pouvez installer un nombre illimité de ces

dispositifs sous la forme d'un dispositif TAP réseau ou en tant que sous-réseau pour collecter les données de paquets brutes.

Si vous n'avez pas de périphérique de capture de paquet connecté, vous pouvez charger manuellement les fichiers de capture de paquet à l'aide de l'interface utilisateur ou de FTP.

Chapitre 3. Présentation de l'installation de QRadar Incident Forensics

Vous pouvez installer le logiciel QRadar Incident Forensics sur votre propre dispositif ou sur un dispositif virtuel. Le logiciel QRadar Incident Forensics est installé sur les dispositifs QRadar Incident Forensics.

QRadar Incident Forensics doit être installé sur un système d'exploitation Red Hat Enterprise Linux.

Sélection de l'ID du dispositif

Pour la plupart des configurations de QRadar Incident Forensics, vous devez installer au moins deux images ISO :

- QRadar Console

  Les produits QRadar utilisent la même image du logiciel d'installation. La *clé d'activation* détermine le type de dispositif et les composants à installer. Lorsque vous entrez la clé d'activation, vous êtes invité à identifier le type de dispositif. Vous devez installer QRadar Console.
- 6000 QRadar Incident Forensics Processor (hôte géré)

  En raison de contrôles lors de l'exportation, les composants QRadar Incident Forensics sont installés à partir d'une autre image ISO. Vous devez installer l'hôte géré QRadar Incident Forensics et le configurer pour établir une connexion avec QRadar Console

Pour les installations globales, vous devez uniquement installer l'image ISO 6100 QRadar Incident Forensics et sélectionner le composant QRadar Incident Forensics Standalone.

Lorsque vous installez QRadar Incident Forensics, une clé de licence par défaut vous offre un accès pendant cinq semaines. Avant que la licence n'arrive à expiration, vous devez allouer une clé de licence à votre système.

Etapes d'installation

Pour les installations distribuées, suivez les étapes ci-dessous pour effectuer la procédure d'installation.

1. Passez en revue les configurations matérielle et logicielle requises.
2. Installez le logiciel QRadar Console.
3. Installez l'hôte géré QRadar Incident Forensics.
4. Déployez l'hôte géré QRadar Incident Forensics.
5. Ajoutez des périphériques de capture de paquet.

Clés d'activation et clés de licence

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

Clé d'activation

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

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

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

Clé de licence

Votre système inclut une clé de licence temporaire qui vous permet d'accéder au logiciel QRadar pendant cinq semaines. Après l'installation et avant l'expiration de la clé de licence, vous devez ajouter les licences achetées.

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 d'exploitation de votre système. Vous devez appliquer vos clés de licence avant l'expiration de votre licence par défaut.

Accessoires matériels et logiciels de bureau prérequis pour les installations de QRadar

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

Accessoires matériels

Assurez-vous que vous avez accès aux composants matériels suivants :

- Moniteur et clavier
- Alimentation de secours (UPS) pour tous les systèmes stockant des données, tels que QRadar Console, les composants processeur d'événements ou les composants QRadar QFlow Collector

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

Configuration logicielle requise pour le système de bureau

Assurez-vous que les applications ci-dessous sont installées sur tous les systèmes de bureau qui vous servent à accéder à l'interface utilisateur des produits QRadar :

- Java™ Runtime Environment (JRE) version 1.7 ou IBM 64-bit Runtime Environment for Java V7.0
- Adobe Flash version 10.x

Navigateurs Web pris en charge

Le tableau suivant répertorie les navigateurs Web pris en charge :

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

Navigateur Web	**Versions prises en charge**
Mozilla Firefox	38.0 Extended Support Release
Microsoft Internet Explorer 32 bits ou 64 bits, avec le mode document ou le mode navigateur activé.	10.0
Microsoft Internet Explorer 64 bits avec le mode Microsoft Edge activé.	11.0
Google Chrome	Version 46

Si vous utilisez Microsoft Internet Explorer, vous devez activer le mode document et le mot navigateur :

1. Dans le navigateur Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre Outils de développement.
2. Cliquez sur **Mode navigateur** et sélectionnez la version de votre navigateur Web.
3. Cliquez sur **Mode document**.
   - Pour Internet Explorer V9.0, sélectionnez **Normes d'Internet Explorer 9**.
   - Pour Internet Explorer V10.0, sélectionnez **Normes d'Internet Explorer 10**.

Ports ouverts nécessaires pour la communication entre les hôtes QRadar Incident Forensics

Le tableau répertorie les ports devant être ouverts entre les hôtes QRadar Incident Forensics :

Tableau 2. Ports ouverts entre les hôtes

Port	**Description**
443	Requis pour l'analyse d'artefact
28080	Requis pour la recherche distribuée

Chapitre 4. Installations du logiciel QRadar Incident Forensics sur votre propre dispositif

Pour réussir l'installation d'IBM Security QRadar Incident Forensics sur votre propre dispositif, vous devez installer le système d'exploitation Red Hat Enterprise Linux, le composant QRadar Console et l'hôte géré QRadar Incident Forensics.

Pour les nouvelles installations de logiciels qui intègrent QRadar Incident Forensics à IBM Security QRadar, vous installez deux fichiers ISO :

- QRadar

  Un fichier ISO est utilisé pour installer chaque produit QRadar sauf pour QRadar Incident Forensics. La clé d'activation entrée détermine le type de dispositif QRadar installé.
- QRadar Incident Forensics

  Cette image ISO contient QRadar Incident Forensics Processor et QRadar Incident Forensics Standalone. Vous devez installer QRadar Incident Forensics Processor.

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

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

Le tableau ci-dessous décrit la configuration système requise :

Tableau 3. Configuration système requise pour les installations RHEL sur votre propre dispositif

Condition requise	Détails
Version de logiciel prise en charge	Version 6.7
Version de bits	64 bits
Disques de démarrage	Non pris en charge
Mémoire (vive) pour le processeur Forensics	128 Go au minimum **Important :** Vous devez mettre à niveau votre mémoire système avant d'installer QRadar.
Espace disque libre pour le processeur Forensics	5 % minimum de l'espace disque total **Important :** Pour des performances optimales, assurez-vous qu'un espace correspondant à 2 à 3 fois l'espace disque minimal est disponible.

Tableau 3. Configuration système requise pour les installations RHEL sur votre propre dispositif (suite)

Condition requise	Détails
Configuration de pare-feu	Activée pour WWW (http, https) Activée pour 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 a fenêtre System Setup.

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

Propriétés des partitions du système d'exploitation Linux pour les installations QRadar sur votre propre dispositif

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

Utilisez les valeurs du tableau ci-après pour vous guider lorsque vous recréez le partitionnement sur le système d'exploitation Red Hat Enterprise Linux.

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

Tableau 4. Guide de partitionnement pour RHEL

Partition	Description	Point de montage	Type de système de fichiers	Taille	Principal	SDA ou SDB
`/boot`	Fichiers d'amorçage système	`/boot`	EXT4	200 Mo	Oui	SDA

Tableau 4. Guide de partitionnement pour RHEL (suite)

Partition	Description	Point de montage	Type de système de fichiers	Taille	Principal	SDA ou SDB
swap	Utilisé comme mémoire lorsque la mémoire vive est saturée.	empty	swap	Systèmes dotés de 4 à 8 Go de mémoire vive. La taille de la partition de permutation doit correspondre à la quantité mémoire vive. Systèmes dotés de 8 à 24 Go de mémoire vive. Configurez la taille de la partition de permutation en attribuant une valeur correspondant à 75 % de la mémoire vive, avec une valeur minimale de 8 Go et une valeur maximale de 24 Go.	Non	SDA
/	Zone d'installation pour QRadar, le système d'exploitation et les fichiers associés.	/	EXT4	20000 Mo	Non	SDA
/store/tmp	Zone de stockage des fichiers temporaires QRadar	/store/tmp	EXT4	20000 Mo	Non	SDA
/var/log	Zone de stockage des fichiers QRadar et des journaux système	/var/log	EXT4	20000 Mo	Non	SDA
/store	Zone de stockage des données et des fichiers de configuration QRadar	/store	XFS	[1]Sur les dispositifs de type Console : environ 80 % de l'espace de stockage disponible. Sur les hôtes gérés qui ne sont pas des collecteurs QFlow ou des collecteurs d'événements stockés et réacheminés : environ 90 % de l'espace de stockage disponible.	Non	SDA S'il y a deux disques, SDB

Tableau 4. Guide de partitionnement pour RHEL (suite)

Partition	Description	Point de montage	Type de système de fichiers	Taille	Principal	SDA ou SDB
/store/transient	Zone de stockage du curseur de base de données ariel	/store/transient	XFS sur les consoles EXT4 sur les hôtes gérés	[1]Sur les dispositifs de type Console : 20 % de l'espace de stockage disponible. Sur les hôtes gérés qui ne sont pas des collecteurs QFlow ou des collecteurs d'événements de stockage et de transfert : 10 % de l'espace de stockage disponible.	Non	SDA S'il y a deux disques, SDB

[1] Ensemble, /store et /store/transient représentent 100 % de l'espace disque restant après la création des cinq premières partitions.

Restrictions

Les mises à niveau ultérieures du logiciel risquent d'échouer si vous reformatez l'une des partitions suivantes ou les sous-partitions associées :

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

Installation de RHEL sur votre propre dispositif

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

Procédure

1. Copiez le DVD ISO du système d'exploitation Red Hat Enterprise Linux sur l'un des périphériques de stockage suivants :
   - DVD
   - Clé USB amorçable

     Pour plus d'informations sur la création d'une clé USB amorçable, voir *IBM Security QRadar - Guide d'installation*.
2. Insérez le périphérique de stockage dans votre dispositif et redémarrez le dispositif.
3. Dans le menu de démarrage, sélectionnez l'une des options suivantes.
   - Sélectionnez la clé USB ou le lecteur DVD comme option d'amorçage.
   - Pour effectuer une installation sur un système prenant en charge Extensible Firmware Interface (EFI), vous devez démarrer le système en mode propriétaire.
4. Lorsque vous y êtes invité, connectez-vous au système comme utilisateur principal.

5. Pour empêcher un problème de désignation des adresses d'interface Ethernet, dans la page Welcome, appuyez sur la touche de tabulation et, à la fin de la ligne `Vmlinuz initrd=initrd.image`, ajoutez `biosdevname=0`.
6. Suivez les instructions de l'assistant d'installation pour effectuer l'installation :
   a. Sélectionnez l'option **Basic Storage Devices**.
   b. Lorsque vous configurez le nom d'hôte, la propriété **Hostname** peut contenir des lettres, des nombres et des tirets.
   c. Lorsque vous configurez le réseau, dans la fenêtre Network Connections, sélectionnez **System eth0**, puis cliquez sur **Edit** et sélectionnez **Connect automatically**.
   d. Sous l'onglet **IPv4 Settings**, dans la liste **Method**, sélectionnez **Manual**.
   e. Dans la zone **DNS servers**, entrez une liste de valeurs séparées par des virgules.
   f. Sélectionnez l'option **Create Custom Layout**.
   g. Configurez `EXT4` pour le type de système de fichiers pour la partition `/boot`.
   h. Reformatez la partition de permutation avec le type de système de fichiers de permutation.
   i. Sélectionnez **Basic Server**.
7. Une fois l'installation terminée, cliquez sur **Reboot**.
8. Assurez-vous que les interfaces réseau intégrées sont nommées `eth0`, `eth1`, `eth2` et `eth3`.

Que faire ensuite

Chapitre 7, «Installation de QRadar Console», à la page 23

Chapitre 5. Installation du logiciel QRadar Incident Forensics sur un dispositif QRadar Incident Forensics

Le système d'exploitation Red Hat Enterprise Linux et le logiciel QRadar sont préinstallés sur les dispositifs IBM Security QRadar Incident Forensics.

Pour les nouvelles installations de logiciels qui intègrent QRadar Incident Forensics à IBM Security QRadar, vous devez configurer deux fichiers ISO préchargés :

- QRadar

  Un fichier ISO est utilisé pour installer chaque produit QRadar sauf pour QRadar Incident Forensics. La clé d'activation indiquée détermine le type de dispositif QRadar installé.
- QRadar Incident Forensics

  Cette image ISO contient QRadar Incident Forensics Processor et QRadar Incident Forensics Standalone. Vous devez installer QRadar Incident Forensics Processor.

Pour les nouvelles installations de logiciels où seules les fonctionnalités Forensics sont nécessaires, installez QRadar Incident Forensics Standalone à partir du fichier ISO QRadar Incident Forensics.

Chapitre 6. Installations de dispositifs virtuels pour QRadar Incident Forensics

Vous pouvez installer IBM Security QRadar Incident Forensics sur un dispositif virtuel. Veillez à utiliser un dispositif virtuel pris en charge qui respecte la configuration système requise minimale.

Un dispositif virtuel est un système QRadar Incident Forensics, qui comprend le logiciel QRadar Incident Forensics installé sur un ordinateur virtuel VMWare ESX.

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.

Processus d'installation

Pour installer un dispositif virtuel, exécutez les tâches ci-dessous dans cet ordre :

__ • Créez un ordinateur virtuel.

__ • Installez le logiciel IBM Security QRadar Incident Forensics sur l'ordinateur virtuel.

__ • Si vous installez QRadar Incident Forensics Processor, ajoutez votre dispositif virtuel au déploiement.

Configuration système requise pour les dispositifs virtuels

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

Tableau 5. Configuration requise pour les dispositifs virtuels.

Condition requise	Description
Client VMware	VMware ESXi version 5.0 VMware ESXi version 5.1 VMware ESXi version 5.5 Pour plus d'informations sur les clients VMWare, consultez le site web VMware (www.vmware.com)
Taille de disque virtuel	256 Go minimum **Important :** Pour optimiser vos performances, assurez-vous qu'un espace correspondant à 2 à 3 fois l'espace disque minimal est disponible.

Création de votre ordinateur virtuel

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

Procédure

1. Depuis VMware vSphere Client, sélectionnez **Fichier** > **Nouveau** > **Machine virtuelle**.
2. Ajoutez les **Nom et l'emplacement**, et sélectionnez le **Magasin de données** pour la nouvelle machine virtuelle.
3. Pour faciliter votre choix, servez-vous des étapes ci-dessous comme référence :
   a. Dans le volet **Configuration** de l'assistant Créer une nouvelle machine virtuelle, sélectionnez **Personnalisée**.
   b. Dans le volet **Nouvelle machine virtuelle**, sélectionnez **Machine virtuelle de version 7**.
   c. Pour le **système d'exploitation**, sélectionnez **Linux** et **Red Hat Enterprise Linux 6 (64 bits)**.
   d. Dans la page **CPUs**, configurez le nombre de processeurs virtuels que vous souhaitez avoir sur l'ordinateur virtuel : Sélectionnez 40 ou plus.
   e. Dans la zone **Taille de la mémoire**, entrez ou sélectionnez la quantité de mémoire RAM requise pour votre déploiement. Sélectionnez 128 Go ou plus.
   f. Utilisez le tableau ci-dessous pour configurer les connexions réseau.

Tableau 6. 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 7. Paramètres de taille de disque virtuel et paramètres de règles de mise à disposition

Propriété	Option
Capacité	2 ou supérieure (To)
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 le logiciel QRadar sur la machine virtuelle.

Installation du logiciel QRadar Incident Forensics sur un ordinateur virtuel

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

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

Procédure

1. Dans le volet de navigation de gauche de votre VMware vSphere Client, sélectionnez votre ordinateur virtuel.
2. Dans le volet de droite, cliquez sur l'onglet **Résumé**.
3. Dans le volet **Commandes**, cliquez sur **Modifier les paramètres**.
4. Dans le volet de gauche de la fenêtre des **propriétés de machine virtuelle**, cliquez sur **Lecteur CD/DVD 1**.
5. Dans le volet **Statut du périphérique**, cochez la case **Connecter à mise sous tension**.
6. Dans le volet **Type de Périphérique**, sélectionnez **Fichier ISO banque de données** et cliquez sur **Parcourir**.
7. Dans la fenêtre Parcourir la BD, localisez et sélectionnez le fichier ISO du produit, cliquez sur **Ouvrir**, puis sur **OK**.
8. Une fois l'image ISO du produit installée, cliquez avec le bouton droit de la souris sur votre machine virtuelle, puis cliquez sur **Alimentation** > **Mettre sous tension.**
9. Connectez-vous à l'ordinateur virtuel en entrant `root` comme nom d'utilisateur.

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

    Conseil : Appuyez sur la barre d'espacement pour parcourir le document.
11. Dans la page de **sélection de l'ID du dispositif**, choisissez le composant QRadar Incident Forensics à installer.
    - Pour une installation distribuée, sélectionnez **6000 QRadar Incident Forensics Processor**.
    - Pour des déploiements autonomes, sélectionnez **6100 QRadar Incident Forensics Standalone**.
12. Pour le type de configuration, sélectionnez **Normal**.
13. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.

    Le tableau ci-dessous contient des descriptions et des remarques pour vous aider à configurer l'installation.

Tableau 8. Description des paramètres réseau

Paramètre réseau	Description
Nom d'hôte	Nom de domaine complet qualifié
Adresse de serveur DNS secondaire	Facultatif
Adresse IP publique utilisant Network Address Translation (NAT)	Non pris en charge
Nom du serveur de messagerie	Si vous ne disposez pas d'un serveur de messagerie, utilisez `localhost`.
Mot de passe root	Le mot de passe doit répondre aux critères suivants : • Il doit contenir au moins 5 caractères. • Il ne doit pas contenir d'espaces. • Il peut inclure les caractères spéciaux suivants : @, #, ^ et *.

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

Que faire ensuite

Si vous n'installez pas IBM Security QRadar Incident Forensics Standalone, voir Chapitre 9, «Ajout d'un hôte géré QRadar Incident Forensics à QRadar Console», à la page 27.

Chapitre 7. Installation de QRadar Console

Pour les installations distribuées, installez QRadar Console sur un dispositif et l'hôte géré IBM Security QRadar Incident Forensics sur un autre dispositif.

Restriction : Lors du déploiement, les logiciels de tous les dispositifs doivent posséder un niveau de version et de correctif identique. Les déploiements qui utilisent des versions de logiciel différentes ne sont pas pris en charge.

Avant de commencer

Veillez à respecter la configuration requise suivante :

- Le matériel requis est installé.
- Un clavier et un moniteur sont connectés via la connexion VGA.
- La clé d'activation est disponible.
- Si vous souhaitez configurer des interfaces réseau de liaison, voir www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).

Procédure

1. Pour les installations effectuées dans votre propre configuration matérielle ou sur des machines virtuelles, ajoutez l'image ISO QRadar Console au répertoire root.
   a. Créez le répertoire `/media/dvd` en entrant la commande suivante :
      `mkdir /media/dvd`
   b. Montez l'image QRadar Console ISO en entrant la commande suivante :
      `mount -o loop <chemin_ISO_QRadar> /media/dvd`
2. Utilisez le script de configuration pour commencer l'installation.
   a. Changez de répertoire de travail en entrant la commande : `cd /media/dvd`
   b. Démarrez le script de configuration en entrant la commande : `setup.sh`
3. Suivez les instructions de l'assistant d'installation.
   - A l'invite du système, utilisez la zone **de saisie de la clé d'activation** pour entrer la chaîne alphanumérique composée de 24 chiffres et de 4 parties fournie par IBM.

     La lettre I et le nombre 1 (un) sont traités de la même façon. La lettre O et le nombre 0 (zéro) sont traités de la même façon.
   - Si vous n'avez pas de serveur de messagerie, entrez `localhost` dans la zone définissant le **nom du serveur de messagerie** dans la page de **saisie des informations réseau à utiliser**.
   - Dans la zone définissant le **mot de passe root**, créez un mot de passe remplissant les critères suivants :
     – Il doit contenir au moins 5 caractères.
     – Il ne doit pas contenir d'espaces.
     – Il peut inclure les caractères spéciaux suivants : @, #, ^ et *.

   La procédure d'installation peut prendre quelques minutes.
4. 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 importez votre clé de licence.
g. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.
h. Dans la liste de licences, sélectionnez un système, puis cliquez sur **Allouer un système à la licence**.

Que faire ensuite

Vous pouvez maintenant installer QRadar Incident Forensics.

Chapitre 8. Installation de QRadar Incident Forensics

Pour les installations distribuées, installez QRadar Console sur un dispositif et l'hôte géré IBM Security QRadar Incident Forensics (QRadar Incident Forensics Processor) sur un autre dispositif. Pour les déploiements autonomes, installez uniquement le composant QRadar Incident Forensics Standalone.

Restriction : Lors du déploiement, les logiciels de tous les dispositifs doivent posséder un niveau de version et de correctif identique. Les déploiements qui utilisent des versions de logiciels différentes ne sont pas pris en charge.

Avant de commencer

Veillez à respecter la configuration requise suivante :

__ • Le matériel requis est installé.

__ • Un clavier et un moniteur sont connectés via la connexion VGA.

__ • La clé d'activation est disponible.

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

Procédure

1. Pour les installations effectuées dans votre propre configuration matérielle ou sur des machines virtuelles, ajoutez l'image ISO QRadar Incident Forensics au répertoire root.
   a. Créez le répertoire `/media/dvd` en entrant la commande suivante :
      `mkdir /media/dvd`
   b. Montez l'image QRadar Console ISO en entrant la commande suivante :
      `mount -o loop <image_ISO_QRadar_Incident_Forensics>/media/dvd`
2. Utilisez le script de configuration pour commencer l'installation.
   a. Changez de répertoire de travail en entrant la commande : `cd /media/dvd`
   b. Démarrez le script de configuration en entrant la commande : `setup.sh`
3. Suivez les instructions de l'assistant d'installation.

   Dans la page de **sélection de l'ID du dispositif**, choisissez le composant QRadar Incident Forensics à installer.
   - Pour une installation distribuée, sélectionnez **6000 QRadar Incident Forensics Processor**
   - Pour des déploiements autonomes, sélectionnez **6100 QRadar Incident Forensics Standalone**

   Restriction : Les options de configuration suivantes ne sont pas prises en charge pour QRadar Incident Forensics :
   - Dans la page Choose the type of setup, l'option **HA Recovery Setup**
   - Dans la page Select if you want to use bonded interface configuration mode, l'option **Use bonded interface configuration mode**

   Si vous installez QRadar Incident Forensics Processor, la procédure d'installation peut prendre plusieurs minutes.
4. Appliquez la 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 le mot de passe du compte utilisateur root.

b. Cliquez sur Connexion.

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 liste **Afficher**, sélectionnez **Licences** et chargez la clé de licence.

g. Sélectionnez la licence disponible et cliquez sur **Allouer un système à la licence**.

h. Dans la liste de licences, sélectionnez une licence et cliquez sur **Allouer une licence au système**.

Vous devez allouer deux clés de licence au dispositif IBM Security QRadar Incident Forensics Standalone. Une licence est destinée à QRadar Incident Forensics Standalone et l'autre permet d'accéder à l'onglet **Forensics**.

Que faire ensuite

Déployez l'hôte géré QRadar Incident Forensics Processor. Pour plus d'informations, voir Chapitre 9, «Ajout d'un hôte géré QRadar Incident Forensics à QRadar Console», à la page 27.

Chapitre 9. Ajout d'un hôte géré QRadar Incident Forensics à QRadar Console

Pour les installations distribuées, vous pouvez ajouter IBM Security QRadar Incident Forensics Processor en tant qu'hôte géré au composant QRadar Console.

Un *hôte géré* désigne n'importe quel dispositif QRadar qui n'est pas utilisé comme console lors du déploiement. Pour distribuer le traitement, vous pouvez ajouter plusieurs composants QRadar Incident Forensics Processor en tant qu'hôte géré.

Restriction : L'utilisation de l'éditeur de déploiement pour ajouter ou supprimer des hôtes gérés QRadar Incident Forensics n'est pas prise en charge. Vous devez utiliser l'outil Gestion du système et de la licence.

Avant de commencer

Vous devez d'abord installer le logiciel QRadar Console. Pour plus d'informations, voir Chapitre 7, «Installation de QRadar Console», à la page 23.

Procédure

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

   `https://`*`Adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe correspond au mot de passe du compte utilisateur root indiqué lors de l'installation.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. Dans la table des hôtes, cliquez sur l'hôte QRadar Console et sélectionnez > **Actions de déploiement** > **Ajouter l'hôte**.
5. Entrez les informations du dispositif QRadar Incident Forensics Processor, puis cliquez sur **Ajouter**.

   Restriction : Les propriétés **Chiffrer l'hôte** et **Conversion d'adresses réseau** ne sont pas prises en charge.
6. Dans la barre de menus de l'onglet **Admin**, cliquez sur **Déployer les changements**.
7. Actualisez le navigateur Web.

   L'onglet **Forensics** est désormais visible.

Que faire ensuite

Vous pouvez ajouter un périphérique IBM Security QRadar Packet Capture au composant QRadar Incident Forensics Processor. Pour plus d'informations, voir «Ajout de périphériques de capture de paquet aux hôtes QRadar Incident Forensics», à la page 32.

Suppression d'un hôte géré QRadar Incident Forensics

Si vous souhaitez modifier les paramètres de configuration réseau ou que vous ne parvenez pas à visualiser l'onglet **Forensics**, vous pouvez supprimer l'hôte géré QRadar Incident Forensics (IBM Security QRadar Incident Forensics Processor) du déploiement QRadar. Si l'hôte géré QRadar Incident Forensics était chargé des procédures de reprise Forensics, les données sont perdues lorsque vous ajoutez à nouveau QRadar Incident Forensics Processor.

Si vous ne supprimez pas l'hôte géré QRadar Incident Forensics mais qu'il ne répond plus provisoirement en raison d'une panne de courant ou à la suite d'un autre événement, les travaux de l'hôte géré restent planifiés et sont traités lorsque le fonctionnement de l'hôte est rétabli.

Restriction : L'utilisation de l'éditeur de déploiement pour ajouter ou supprimer des hôtes gérés QRadar Incident Forensics n'est pas prise en charge. Vous devez utiliser l'outil Gestion du système et de la licence.

Procédure

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

   `https://`*`Adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe correspond au mot de passe du compte utilisateur root indiqué lors de l'installation.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. Dans la table des hôtes, cliquez sur l'hôte QRadar Incident Forensics Processor que vous souhaitez supprimer et sélectionnez > **Actions de déploiement** > **Supprimer l'hôte**.
5. Dans la barre de menus de l'onglet **Admin**, cliquez sur **Déployer les changements**.
6. Actualisez le navigateur Web.

Chapitre 10. Connexions entre les périphériques de capture de paquet et QRadar Incident Forensics

Pour extraire les données de capture de paquet, vous devez connecter un ou plusieurs périphériques de capture de paquet à un hôte géré IBM Security QRadar Incident Forensics ou à un composant QRadar Incident Forensics Standalone. Si vous n'avez pas de périphérique de capture de paquet connecté, vous pouvez charger manuellement les fichiers de capture de paquet à l'aide de l'interface utilisateur ou de FTP.

Système maître de capture de paquet

En fonction des besoins de votre réseau et de la procédure de capture de paquet, vous pouvez connecter jusqu'à cinq périphériques de capture de paquet à un dispositif QRadar Incident Forensics. Lorsque vous soumettez une procédure de reprise, des travaux distincts sont soumis pour chaque périphérique de capture de paquet sur chaque dispositif QRadar Incident Forensics. Par exemple, si vous installez deux hôtes gérés QRadar Incident Forensics et que chacun d'eux inclut deux captures de paquet, quatre travaux sont soumis.

Les diagrammes ci-après indiquent que vous pouvez connecter plusieurs périphériques de capture de paquet à un hôte géré QRadar Incident Forensics (QRadar Incident Forensics Processor) ou à des dispositifs QRadar Incident Forensics Standalone.

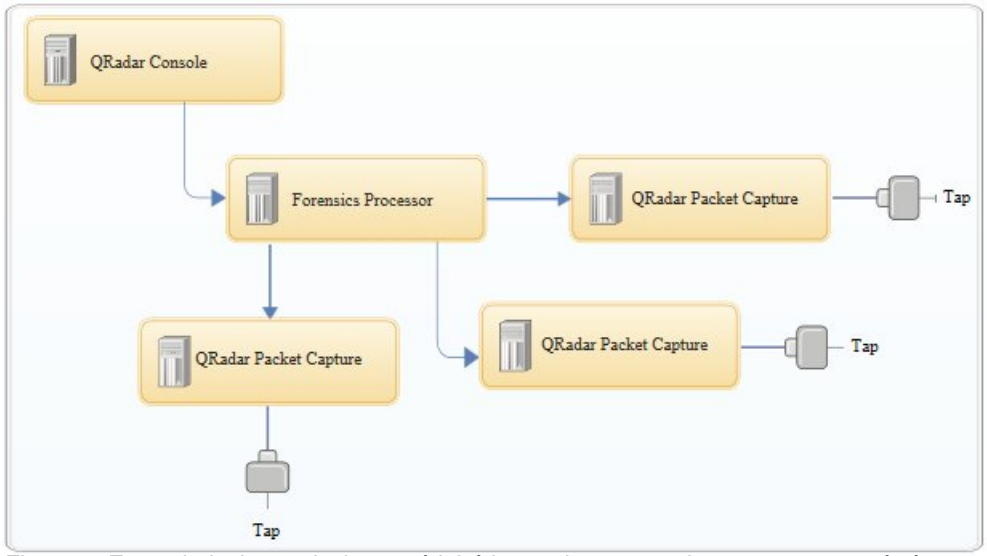


Figure 4. Exemple incluant plusieurs périphériques de capture de paquet connectés à un hôte géré QRadar Incident Forensics

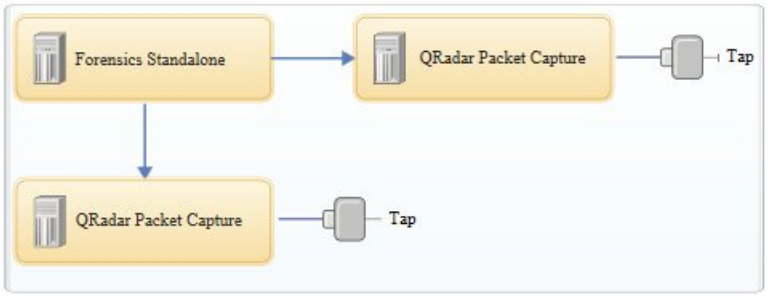
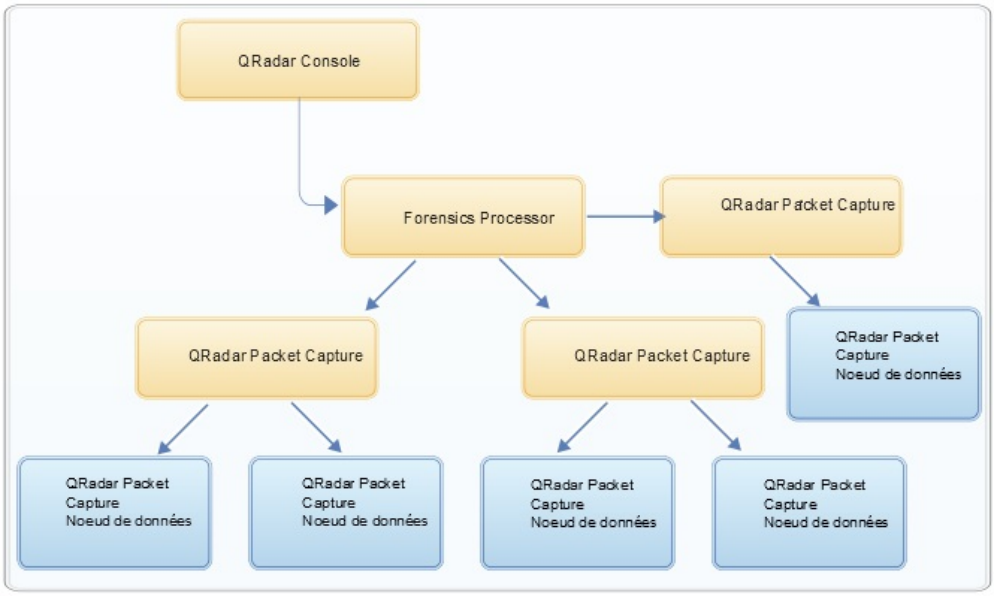


Figure 5. Exemple incluant plusieurs périphériques de capture de paquet connectés à un hôte QRadar Incident Forensics Standalone.

Dispositifs Noeud de données QRadar Packet Capture

Pour disposer de capacités de stockage supplémentaires, vous pouvez connecter jusqu'à deux dispositifs Noeud de données QRadar Packet Capture à chaque système QRadar Packet Capture maître. Chaque dispositif Noeud de données PCAP fournit 37 To d'espace de stockage supplémentaire.



Après avoir connecté des dispositifs Noeud de données QRadar Packet Capture au système maître, vous pouvez configurer le cluster dans l'interface utilisateur QRadar Packet Capture.

Pour plus d'informations sur les connexions physiques reliant le dispositif maître au dispositif Noeud de données QRadar Packet Capture, reportez-vous au document *QRadar Packet Capture - Aide-mémoire*. Pour plus d'informations sur la configuration du cluster de capture de paquet, reportez-vous au document *QRadar Packet Capture - Guide d'utilisation*.

Installation du logiciel QRadar Packet Capture sur votre propre dispositif

Pour réussir une installation de IBM Security QRadar Packet Capture sur votre propre dispositif, vous devez installer le système d'exploitation Red Hat Enterprise Linux et le logiciel QRadar Packet Capture. Vous devez également vérifier que le dispositif respecte la configuration système requise.

Important : Le système où le logiciel QRadar Packet Capture est installé doit être dédié à QRadar Packet Capture. N'installez pas de modules RPM non approuvés par IBM. L'installation de modules RPM non approuvés risque de générer des erreurs de dépendance lors de la mise à niveau et des problèmes de performances lors du déploiement. N'utilisez pas YUM pour mettre à jour le système d'exploitation ou installer des logiciels non approuvés sur des systèmes QRadar Packet Capture.

Restriction : L'installation de logiciels sur une machine virtuelle n'est pas prise en charge.

Avant de commencer

Vérifiez que le dispositif respecte la configuration système suivante :

Tableau 9. Configuration système pour une installation du logiciel QRadar Packet Capture

Spécification	Description
Processeurs	Processeurs Intel E5 Series à 6 coeurs ou plus V2 et V3. Doit prendre en charge les normes Intel AES et AVX présentées par Intel en 2011.
Mémoire	16 Go
Contrôleur RAID et magasin de capture et d'extraction	Contrôleur RAID 0 (segment) pour quatre disques durs minimum pouvant atteindre chacun des performances de 72000 RPM avec au moins 1 To par disque d'entreprise SATA ou SAS compatible RAID.
Disque du système d'exploitation	Disque dur d'entreprise SATA ou SAS de 500 Go minimum, pouvant atteindre 7200 RPM
Système d'exploitation	Red Hat Enterprise Linux version 6.5
Adaptateur serveur quatre ports	Adaptateur Intel E1G44ET2BLK Ethernet PCI Express quatre ports http://ark.intel.com/products/49187/Intel-Gigabit-ET2-Quad-Port-Server-Adapter prenant en charge un port de capture Contrôleur Intel 82576 Gigabit Ethernet http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller

Procédure

1. Insérez le disque du système d'exploitation Red Hat Enterprise Linux dans votre dispositif et redémarrez-le.
2. Suivez les instructions de l'assistant d'installation pour effectuer l'installation :

a. Sélectionnez l'option **Basic Storage Devices**.
b. Lorsque vous configurez le nom d'hôte, la propriété **Hostname** peut contenir des lettres, des nombres et des tirets.
c. Sous l'onglet **IPv4 Settings**, dans la liste **Method**, sélectionnez **Manual**.
d. Dans la page Which type of installation would you like, sélectionnez **Use All Space**, puis choisissez la partition la plus petite (partition d'amorçage) sur le système d'exploitation où l'installation doit être effectuée.
e. Sélectionnez uniquement l'option **Base System** pour l'installation.

3. Une fois l'installation terminée, cliquez sur **Reboot**.
4. Copiez le fichier SFS QRadar Packet Capture sur votre dispositif.
5. Montez le fichier SFS QRadar Packet Capture.
   a. Créez le répertoire `/tmp/qpc_install` en tapant la commande suivante :
      ```
      mkdir -p /tmp/qpc_install
      ```
   b. Montez le fichier SFS QRadar Packet Capture en tapant la commande suivante :
      ```
      mount -o loop -t squashfs <fichier_QRadar_Packet_Capture.sfs>
      /tmp/qpc_install
      ```
   c. Accédez au répertoire `/tmp/qpc_install`.
      ```
      cd /tmp/qpc_install
      ```
6. Pour exécuter le script d'installation, tapez la commande suivante :
   ```
   sh installer.sh
   ```

Ajout de périphériques de capture de paquet aux hôtes QRadar Incident Forensics

Pour permettre aux examinateurs d'accéder aux informations de capture de paquet, vous pouvez connecter jusqu'à cinq périphériques de capture à un hôte géré IBM Security QRadar Incident Forensics ou à un hôte IBM Security QRadar Incident Forensics Standalone. Les périphériques de capture de paquet connectés traitent les fichiers capturés pour les reprises Forensics.

Si vous n'avez pas de périphérique de capture de paquet connecté, vous pouvez charger manuellement les fichiers de capture de paquet à l'aide de l'interface utilisateur ou de FTP.

Restriction : L'utilisation de l'éditeur de déploiement pour ajouter des périphériques de capture de paquet n'est pas prise en charge. Vous devez utiliser l'outil Gestion du système et de la licence.

Avant de commencer

Vous devez installer et déployer un hôte géré QRadar Incident Forensics ou installer un hôte QRadar Incident Forensics Standalone. Pour plus d'informations, voir Chapitre 8, «Installation de QRadar Incident Forensics», à la page 25 et Chapitre 9, «Ajout d'un hôte géré QRadar Incident Forensics à QRadar Console», à la page 27.

Le diagramme interactif ci-dessous présente les principales étapes de la procédure d'installation en mode distribué. La procédure d'installation est identique pour les déploiements autonomes mais vous ne déployez pas d'hôte géré.

Par défaut, le temps universel coordonné (UTC) est affecté au fuseau horaire du périphérique QRadar Packet Capture.

Procédure

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

   `https://`*`Adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe correspond au mot de passe du compte utilisateur root indiqué lors de l'installation.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. Dans la table des hôtes, sélectionnez l'hôte QRadar Incident Forensics Processor (**Type de dispositif** 6000) ou QRadar Incident Forensics Standalone (**Type de dispositif** 6100) et cliquez sur **Actions de déploiement** > **Modifier l'hôte géré**
5. Cliquez sur **Gestion des composants**.
6. Pour ajouter des périphériques de capture de paquet, cliquez sur l'icône Ajouter (+) et entrez les informations sur le périphérique.

   Conseil : Le nom d'utilisateur par défaut du périphérique QRadar Packet Capture est `continuum`.
7. Cliquez sur **Sauvegarder**.

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

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

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

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

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

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

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

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

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

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de service 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.

Les termes ci-dessous sont des marques d'autres sociétés :

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

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

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

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

Les autres noms de sociétés, produits ou services sont déposés et appartiennent à leurs propriétaires respectifs.

Remarques sur les règles de confidentialité

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

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

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

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

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