IBM Security QRadar Incident Forensics
Version 7.2.3

Guide d'installation

GC43-0870-01

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 19.

Deuxième édition - Juillet 2014

Réf. US : GC27-6507-01

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 systèmesQRadar 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 (en anglais) (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 être inclus dans une solution de sécurité complète, qui implique forcément d'autres procédures opérationnelles et peuvent nécessiter d'autres systèmes, produits ou services pour une efficacité optimale. 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.

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. Nouveautés concernant les programmes d'installation dans QRadar Incident Forensics V7.2.3

IBM Security QRadar V7.2.3 introduit la prise en charge du traitement réparti des données Forensics.

Traitement réparti des données Forensics

Pour répartir le traitement des données Forensics, vous pouvez ajouter plusieurs hôtes QRadar Incident Forensics secondaires. En savoir plus...

Ajout de plusieurs périphériques de capture aux hôtes QRadar Incident Forensics

Pour accorder aux examinateurs Forensic un accès aux informations de capture de paquet, vous pouvez connecter jusqu'à cinq périphériques de capture à un hôte IBM Security QRadar Incident Forensics. En savoir plus...

Chapitre 2. Présentation de l'installation de QRadar Incident Forensics

Vous installez IBM Security QRadar Incident Forensics sur votre propre dispositif ou sur un dispositif IBM Security QRadar Incident Forensics.

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

Pour une vue unifiée des informations sur les flux, les utilisateurs et les événements et des informations Forensics, vous intégrez QRadar Incident Forensics à QRadar.

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 logicielQRadar 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 :

- Ecran et clavier, ou console série
- Alimentation de secours (UPS) pour tous les systèmes permettant de stocker les données, comme les composants QRadar Console, processeur d'événements ou QRadar QFlow Collector
- Câble d'éliminateur de modem si vous souhaitez connecter le système à une console série

Important : Les produits QRadar prennent en charge les implémentations matérielles RAID (Redundant Array of Independent Disks), mais pas les installations logicielle 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 or IBM 64-bit Runtime Environment for Java V7.0
- Adobe Flash version 10.x

Navigateurs Web pris en charge

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

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

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

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

Navigateur Web	Version prise en charge
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer 32 bits, avec mode document et mode navigateur activés	8.0 9.0
Google Chrome	Version en cours à la date d'édition des produits IBM Security QRadar V7.2.3

Activation du mode document et du mode navigateur dans Internet Explorer

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

Procédure

1. Dans votre navigateur Web Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre des outils de développement.
2. Cliquez sur **Mode navigateur** et sélectionnez la version de votre navigateur Web.
3. Cliquez sur **Mode de document**.
   - Pour Internet Explorer 9.0, sélectionnez **Normes Internet Explorer 9**
   - Pour Internet Explorer 8.0, sélectionnez **Normes Internet Explorer 8**

Installations réparties

Vous pouvez définir des investigations Forensics à l'aide de plusieurs hôtes IBM Security QRadar Incident Forensics et dispositifs IBM Security QRadar Packet Capture.

Chaque hôte QRadar Incident Forensics se trouvant sur le réseau est un noeud. Le noeud connecté directement à QRadar Console est le noeud principal et tous les autres hôtes QRadar Incident Forensics sont des noeuds secondaires.

Le noeud principal et les noeuds secondaires peuvent être connectés à aucun ou plusieurs périphériques de capture.

Chapitre 3. Installations du logiciel QRadar Incident Forensics sur votre propre dispositif

Pour s'assurer que l'installation d'IBM Security QRadar Incident Forensics sur votre propre dispositif, vous devez installer le système d'exploitation Red Hat Enterprise Linux.

Assurez-vous que votre dispositif respecte la configuration système requise pour les déploiements QRadar Incident Forensics.

Conditions requises pour installer 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 2. Configuration système requise pour les installations RHEL sur votre propre dispositif

Condition requise	**Détails**
Version de logiciel prise en charge	Version 6.5
Version de bits	64 bits
Disques KickStart	Non pris en charge
Mémoire (vive) pour le processeur Forensics	64 Go 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.
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.

Propriétés des partitions Linux pour 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-dessous pour vous aider lors de la recréation du 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 3. Guide de partitionnement pour RHEL

Partition	Description	Point de montage	Type de système de fichiers	Taille
`/boot`	Fichiers d'amorçage système	`/boot`	EXT4	200 Mo
swap	Utilisé comme mémoire lorsque la mémoire vive est saturée.	empty	swap	4 094 Mo
/	Zone d'installation pour QRadar Incident Forensics, le système d'exploitation et les fichiers associés.	/	EXT4	40 960 Mo
`/opt`	Zone de stockage pour les données et les fichiers de configuration QRadar Incident Forensics	`/opt`	XFS	Espace disponible restant pour cette partition.

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 contenu du DVD du système d'exploitation Red Hat Enterprise Linux 6.5 ISO sur l'un des périphériques de stockage portables suivants :
   - DVD
   - Clé USB amorçable

     Pour plus d'informations sur la création d'une clé USB amorçable, consultez la note technique *Installing QRadar Using a Bootable USB flash drive* sur le site Web IBM (www.ibm.com/support).
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

«Installation de QRadar Incident Forensics sur un système Red Hat Enterprise Linux existant»

Installation de QRadar Incident Forensics sur un système Red Hat Enterprise Linux existant

Vous pouvez installer IBM Security QRadar Incident Forensics sur un système d'exploitation Red Hat Enterprise Linux existant.

Procédure

1. Ajoutez l'image de QRadar Incident Forensics ISO dans le répertoire principal.
2. Créez le répertoire `/media/dvd` en entrant la commande suivante :
   ```
   mkdir /media/dvd
   ```
3. Montez l'image QRadar Incident Forensics ISO en entrant la commande suivante :
   ```
   mount -o loop <chemin d'accès à QRadar Incident Forensics ISO>
   /media/dvd
   ```
4. 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`
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. La procédure d'installation peut prendre quelques minutes.
6. Redémarrez le serveur QRadar Incident Forensics.

Que faire ensuite

«Intégration de QRadar Incident Forensics à IBM Security QRadar», à la page 10

Intégration de QRadar Incident Forensics à IBM Security QRadar

Intégrez IBM Security QRadar Incident Forensics à IBM Security QRadar pour fournir une vue unifiée des informations sur les flux, les utilisateurs et les événements et des informations Forensics.

Avant de commencer

Vous devez installer IBM Security QRadar en premier. Pour les instructions d'installation, voir *IBM Security QRadar - Guide d'installation*.

Procédure

1. 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.
2. Cliquez sur l'onglet **Admin**.
3. Dans le volet de navigation, cliquez sur **System Configuration**.
4. Dans la section **Forensics**, cliquez sur **Setup Incident Forensics**.
5. Entrez l'adresse IP ou le nom d'hôte du système QRadar Incident Forensics.
6. Entrez le nom d'utilisateur root et le mot de passe utilisés pour accéder au système QRadar Incident Forensics.
7. Cliquez sur **Save Configuration**.
8. Actualisez le navigateur Web. L'onglet **Forensics** est disponible dans la QRadar Console.

Que faire ensuite

Pour répartir le traitement, vous pouvez ajouter plusieurs hôtes QRadar Incident Forensics. Pour plus d'informations, voir «Ajout d'hôtes secondaires», à la page 13.

Chapitre 4. Installation du logiciel QRadar Incident Forensics sur un dispositif QRadar Incident Forensics

Le système d'exploitation Red Hat Enterprise Linux est préinstallé sur les dispositifs IBM Security QRadar Incident Forensics.

Vous pouvez installer le logiciel QRadar Incident Forensics sur un dispositif QRadar Incident Forensics.

Pour une vue unifiée des informations sur les flux, les utilisateurs, les événements et les informations Forensics, vous intégrez QRadar Incident Forensics à IBM Security QRadar.

Installation du logiciel QRadar Incident Forensics sur un dispositif

Installez le logiciel IBM Security QRadar Incident Forensics sur un dispositif QRadar Incident Forensics.

Avant de commencer

Veillez à respecter la configuration requise suivante :

__ • Le matériel requis est installé.

__ • Pour un dispositif QRadar Incident Forensics, un ordinateur portable est connecté au port série à l'arrière du dispositif ou un clavier et un écran sont connectés.

__ • Vous êtes connecté comme utilisateur root.

__ • La clé d'activation est disponible.

Si vous utilisez un ordinateur portable pour vous connecter au système, vous devez utiliser un programme d'émulation de terminal, comme HyperTerminal. Assurez-vous que vous avez défini l'option **Connect Using** sur le port COM approprié du connecteur série. Assurez-vous que vous avez également défini les propriétés suivantes :

Tableau 4. Propriétés de connexion au terminal

Propriété	Paramètre
Bits par seconde	9600
Bits d'arrêts	1
Bits de données	8
Parité	Aucune

Pourquoi et quand exécuter cette tâche

Le tableau ci-dessous décrit les commandes facultatives que vous pouvez utiliser lors de l'installation.

Tableau 5. Commandes facultatives pour l'installation de QRadar Incident Forensics

Commande	Description
HALT	Permet d'éteindre le système. Cette commande est utilisée pour suspendre l'installation avant la configuration. La prochaine fois que le dispositif sera allumé, l'installation reprendra avec la commande SETUP.
SETUP	Permet de reprendre l'installation et d'arrêter le système une fois la configuration terminée.

Procédure

1. Permet d'allumer le système.
2. Entrez SETUP.
3. Pour toutes les installations, 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.
4. Lorsque vous êtes invité à entrer la clé d'activation, entrez la chaîne alphanumérique à 24 caractères, en 4 parties, qu'IBM vous a envoyée.

   La lettre I et le nombre 1 (un) sont traités de la même façon. La lettre O et le nombre 0 (zéro) sont traités de la même façon.
5. Suivez les instructions de l'assistant d'installation pour terminer l'installation.

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

Tableau 6. Description des paramètres réseau

Paramètre réseau	Description
Nom d'hôte	Nom de domaine complet qualifié
Adresse de serveur DNS secondaire	Facultatif
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 *.
Nom de connexion QRadar Forensics	Nom de connexion permettant de se connecter au système QRadar Incident Forensics.

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

«Intégration de QRadar Incident Forensics à IBM Security QRadar», à la page 10

Intégration de QRadar Incident Forensics à IBM Security QRadar

Intégrez IBM Security QRadar Incident Forensics à IBM Security QRadar pour fournir une vue unifiée des informations sur les flux, les utilisateurs et les événements et des informations Forensics.

Avant de commencer

Vous devez installer IBM Security QRadar en premier. Pour les instructions d'installation, voir *IBM Security QRadar - Guide d'installation*.

Procédure

1. 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.
2. Cliquez sur l'onglet **Admin**.
3. Dans le volet de navigation, cliquez sur **System Configuration**.
4. Dans la section **Forensics**, cliquez sur **Setup Incident Forensics**.
5. Entrez l'adresse IP ou le nom d'hôte du système QRadar Incident Forensics.
6. Entrez le nom d'utilisateur root et le mot de passe utilisés pour accéder au système QRadar Incident Forensics.
7. Cliquez sur **Save Configuration**.
8. Actualisez le navigateur Web. L'onglet **Forensics** est disponible dans la QRadar Console.

Que faire ensuite

Pour répartir le traitement, vous pouvez ajouter plusieurs hôtes QRadar Incident Forensics. Pour plus d'informations, voir «Ajout d'hôtes secondaires».

Ajout d'hôtes secondaires

Pour répartir le traitement des données Forensics, vous pouvez ajouter plusieurs hôtes IBM Security QRadar Incident Forensics secondaires.

Vous pouvez configurer une combinaison de 10 hôtes principaux et secondaires. Seulement un seul hôte principal peut être actif.

Avant de commencer

Vous devez ajouter un hôte QRadar Incident Forensics principal en utilisant l'outil **Setup Incident Forensics**. Pour plus d'informations, voir «Intégration de QRadar Incident Forensics à IBM Security QRadar», à la page 10.

Procédure

1. Sous l'onglet **Admin**, cliquez sur **Processor Management**.
2. Dans la section **Secondary Hosts**, cliquez sur **Add**.
3. Cliquez deux fois sur la zone **IP Address** et entrez l'adresse IP de l'hôte QRadar Incident Forensics.
4. Facultatif : Entrez une description pour le périphérique.
5. Cliquez sur **Deploy Changes**.

Chapitre 5. Mise à niveau de QRadar Incident Forensics

Mettez à niveau IBM Security QRadar Incident Forensics pour vous assurer de disposer des fonctions les plus récentes.

Avant de commencer

Veillez à prendre les précautions suivantes :

__ • Vérifiez que vous exécutez Microsoft Internet Explorer 10.0 ou version ultérieure.

Procédure

1. Téléchargez le fichier *<QRadar_Forensics_patchupdate>.sfs* depuis 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_Forensics_patchupdate>.sfs
   /media/updates/
   ```
7. Accédez au répertoire dans lequel vous avez monté le fichier correctif :

   ```
   cd/media/updates
   ```
8. Pour exécuter le programme d'installation des correctifs, entrez la commande suivante :

   ```
   /media/updates/installer
   ```
9. Redémarrez le système pour terminer la mise à niveau.

   Si vous souhaitez vérifier si des problèmes se sont produits lors de la mise à niveau, consultez le journal dans le répertoire `/opt/ibm/forensics/upgrade`.

Chapitre 6. 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 IBM Security QRadar Incident Forensics.

Selon votre réseau et vos besoins en capture de paquet, vous pouvez connecter jusqu'à cinq périphériques de capture de paquet à l'hôte QRadar Incident Forensics principal. En outre, si vous avez réparti des hôtes QRadar Incident Forensics, vous pouvez connecter jusqu'à cinq périphériques de capture de paquets aux hôtes secondaires.

Ajout de périphériques de capture aux hôtes QRadar Incident Forensics

Pour accorder aux examinateurs un accès aux informations de capture de paquet, connectez jusqu'à cinq périphériques de capture à un hôte IBM Security QRadar Incident Forensics.

Avant de commencer

Vous devez ajouter un hôte QRadar Incident Forensics principal en utilisant l'outil **Setup Incident Forensics**. Pour plus d'informations, voir «Intégration de QRadar Incident Forensics à IBM Security QRadar», à la page 10.

Procédure

1. Sous l'onglet **Admin**, cliquez sur **Processor Management**.
2. Ajoutez un périphérique de capture à QRadar Incident Forensics.
   - Pour ajouter un périphérique de capture à l'hôte principal, cliquez sur **Configure**.
   - Pour ajouter un périphérique de capture à un hôte secondaire, sélectionnez un hôte dans le tableau **Secondary Hosts**, puis cliquez sur **Configure**.
3. Cliquez sur **Add**.
4. Cliquez deux fois sur la zone **IP Address** en entrez l'adresse IP du périphérique de capture.
5. Facultatif : Entrez une description pour le périphérique.
6. Tapez un nom d'utilisateur et un mot de passe pour le périphérique de capture.
7. Cliquez sur **Deploy Changes**.

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

Adobe, Acrobat et toutes les marques basées sur Adobe 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 de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans d'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-dessous.

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

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

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

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

Index