IBM QRadar Security Intelligence Platform

Version 7.2.5

Guide de démarrage rapide

Le présent guide explique comment effectuer une installation classique.

Version en langue nationale : Pour obtenir le Guide de démarrage rapide dans d'autres langues, imprimez le PDF spécifique à une langue depuis le support d'installation.

Présentation du produit

Les produits IBM® QRadar Security Intelligence Platform fournissent une architecture unifiée pour intégrer SIEM, la gestion des journaux, la détection des anomalies, Incident Forensics et la gestion des configurations et des vulnérabilités. Ce guide de démarrage rapide fournit des informations concernant l'installation des dispositifs IBM Security QRadar.

1 Étape 1 : Accès aux logiciels et à la documentation

Consultez les Notes sur l'édition relatives au composant QRadar que vous voulez installer.

Téléchargez l'image ISO de votre composant QRadar depuis le site Web IBM FIX Central.

2 Étape 2 : Aperçu des panneaux avant et arrière

Passez en revue les informations relatives aux fonctions du panneau avant et arrière des dispositifs afin de confirmer que la connectivité et les fonctionnalités sont correctes.

Pour plus d'informations sur ces fonctions, voir la section fonctions du panneau avant et arrière.

Sur le panneau arrière de chaque type de dispositif, le connecteur série et les connecteurs Ethernet peuvent être gérés à l'aide du module de gestion intégré. Pour plus de détails sur le module de gestion intégré, consultez le document *Integrated Management Module - Guide d'utilisation*.

3 Étape 3 : Conditions préalables à l'installation

Veillez à respecter la configuration requise suivante :

- Le matériel requis est installé.
- Pour les dispositifs QRadar, 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.

Pour faire en sorte que l'installation d'IBM® Security QRadar® aboutisse sur votre 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. Pour plus d'informations, voir *QRadar Hardware Guide*.

4 Étape 4 : Installation de QRadar SIEM sur votre propre dispositif

Remarque : QRadar Risk Manager et QRadar Incident Forensics requièrent leurs propres licences et doivent être installés sur des dispositifs distincts. QRadar Risk Manager doit être installé en tant qu'hôte géré. QRadar Vulnerability Manager peut être installé sur la même machine que la console, sur une console tout-en-un.

1. Si vous utilisez votre propre dispositif, montez l'image ISO de QRadar :
   a. Créez le répertoire /media/cdrom à l'aide de la commande suivante :

      ```
      mkdir /media/cdrom
      ```

   b. Montez l'image ISO de QRadar en entrant la commande suivante :

      ```
      mount -o loop <chemin image ISO QRadar> /media/cdrom
      ```

   c. Pour commencer l'installation, entrez la commande suivante :

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

2. 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.
3. Pour le type d'installation et de configuration, sélectionnez **Normal**.
4. Sélectionnez le type d'adresse IP.
5. Dans l'assistant, entrez un nom de domaine qualifié complet dans la zone **Nom d'hôte**.
6. Dans la zone **Adresse IP**, entrez une adresse IP statique, ou utilisez l'adresse IP affectée par DHCP.

   Pour plus d'informations sur la configuration d'un hôte principal ou secondaire IPv6, consultez le manuel *IBM Security QRadar High Availability Guide*.
7. Si vous ne disposez pas d'un serveur de messagerie, entrez `localhost` dans la zone **Nom du serveur de messagerie**.
8. Cliquez sur **Terminer**.
9. Dans la zone **Mot de passe root**, créez un mot de passe. Les mots de passe doivent avoir une longueur de 5 caractères au minimum, ils ne doivent pas contenir d'espaces, et peuvent contenir les caractères spéciaux suivants : @, #, ^ et *.
10. Suivez les instructions de l'assistant d'installation pour terminer l'installation. La procédure d'installation peut prendre quelques minutes.

5 Étape 5 : Application de votre clé de licence

1. Connectez-vous à QRadar:

   ```
   https://IP_Address_QRadar
   ```

   Le **nom d'utilisateur** par défaut est `admin`. Le **mot de passe** est le mot de passe du compte de l'utilisateur root.
2. Cliquez sur l'onglet **Admin**.
3. Dans le volet de navigation, cliquez sur **Configuration système**.
4. Cliquez sur l'icône **Gestion du système et de la licence**.
5. Dans la zone de liste **Afficher**, sélectionnez **Licences**, puis envoyez par téléchargement votre clé de licence.
6. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.
7. Dans la liste de licences, sélectionnez une licence, puis cliquez sur **Allouer une licence au système**.

6 Étape 6 : Mise en route

Pour plus d'informations sur l'utilisation de vos composants QRadar, consultez les ressources suivantes :

- Initiation au déploiement de IBM Security QRadar SIEM
- Mise en route d'IBM Security QRadar Risk Manager
- Installations et déploiements de IBM Security QRadar Vulnerability Manager
- Présentation de IBM Security QRadar Incident Forensics

Informations complémentaires

Pour consulter la documentation complète du produit, rendez-vous sur le Knowledge Center d'IBM QRadar Security Intelligence Platform ou sur la page des documents de téléchargement (en anglais).

Référence : CN3VGML

Printed in Ireland