IBM QRadar Security Intelligence Platform

Version 7.3.0

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 une autre langue, imprimez le PDF correspondant depuis le support d'installation.

Présentation du produit

Les produits IBM® QRadar Security Intelligence Platform fournissent une architecture unifiée permettant d'intégrer SIEM, la gestion des journaux, la détection des anomalies, Incident Forensics et la gestion des configurations et des vulnérabilités. Le présent Guide de démarrage rapide contient des informations sur l'installation des dispositifs IBM Security QRadar.

Important : Si QRadar est déjà installé sur votre dispositif, respectez les règles suivantes lors de la création du mot de passe root : le mot de passe doit contenir au moins cinq caractères, sans espaces, et peut contenir les caractères suivants : @, #, ^ et *.

1 Étape 1 : Accès aux logiciels et à la documentation

Consultez les Notes sur l'édition relatives au composant QRadar à installer.

Suivez les instructions des documents de téléchargement (en anglais) (www.ibm.com/support/docview.wss?uid=swg24042706) pour télécharger QRadar depuis IBM Passport Advantage.

2 Étape 2 : Aperçu des panneaux avant et arrière

Passez en revue les informations relatives aux fonctionnalités des panneaux avant et arrière des dispositifs et vérifiez leur connectivité et leur bon fonctionnement.

Pour plus d'informations sur les fonctionnalités des panneaux avant et arrière des dispositifs, consultez la rubrique correspondante.

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, voir le manuel *Integrated Management Module - Guide d'utilisation*.

3 Étape 3 : Conditions préalables à l'installation

La configuration suivante doit être respectée :

- 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 en tant qu'utilisateur root.
- La clé d'activation est disponible.

Pour que l'installation de 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 le manuel *QRadar Hardware Guide*.

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

Remarque : QRadar Risk Manager et QRadar Incident Forensics requièrent leur propre licence 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. Sélectionnez le type de dispositif **Non-Software Appliance**.
3. Sélectionnez-le dans la liste, ou appuyez sur `Ctrl + K` pour entrer la clé d'activation : la chaîne alphanumérique à 24 caractères, en 4 parties, qu'IBM vous a fournie. 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.
4. Sélectionnez le type d'installation **normal**.
5. Configurez la date et l'heure.
6. Sélectionnez le type d'adresse IP.
7. Dans l'assistant, entrez un nom de domaine qualifié complet dans la zone **Hostname**.
8. Dans la zone **IP address**, entrez une adresse IP statique, ou utilisez l'adresse IP affectée par le DHCP.

   Pour plus d'informations sur la configuration d'un hôte principal ou secondaire IPv6, consultez le manuel *IBM Security QRadar High Availability Guide*.
9. Si vous n'avez pas de serveur de messagerie, entrez `localhost` dans la zone **Email server name**.
10. Créez les mots de passe root et administrateur. Les mots de passe doivent contenir au moins 5 caractères, sans espaces, et peuvent contenir les caractères suivants : @, #, ^ et *.
11. Suivez les instructions de l'assistant pour terminer l'installation. Cette procédure 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 celui 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 transférez votre clé de licence.
6. Sélectionnez la licence non allouée et cliquez sur **Allouer un système à la licence**.
7. Dans la liste des licences, sélectionnez-en une, 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 à IBM Security QRadar SIEM
- Initiation à IBM Security QRadar Risk Manager
- Initiation à IBM Security QRadar Vulnerability Manager
- Initiation à IBM Security QRadar Incident Forensics
- Initiation à IBM Security QRadar Packet Capture
- Initiation à IBM QRadar Network Packet Capture

Informations complémentaires

La documentation complète est accessible depuis la page IBM Knowledge Center d'IBM QRadar Security Intelligence Platform. Vous pouvez télécharger la documentation au format PDF depuis la page Accessing IBM Security QRadar documentation.

Printed in Ireland