

Guia de Iniciação Rápida

Este guia apresenta uma instalação típica.

Versão em idioma nacional: para obter o Guia de Iniciação Rápida em outros idiomas, imprima o PDF específico do idioma a partir da mídia de instalação.

Visão geral do produto

Os produtos IBM® QRadar Security Intelligence Platform fornecem uma arquitetura unificada para integrar informações de segurança e gerenciamento de eventos (SIEM), gerenciamento de logs, detecção de anomalias, análise forense de incidentes e gerenciamento de configuração e vulnerabilidades. Este Guia de Iniciação Rápida fornece informações sobre a instalação de dispositivos IBM Security QRadar.

1 Etapa 1: Acessar o software e a documentação



Revise as notas sobre a liberação do componente do QRadar que deseja instalar.

Faça o download da ISO de seu componente do QRadar no website IBM FIX Central.

2 Etapa 2: Revisar os recursos dos painéis dianteiro e traseiro

Revise as informações sobre os recursos dos painéis dianteiro e traseiro dos dispositivos para confirmar a devida conectividade e funcionalidade.

Para obter mais informações sobre os recursos dos painéis dianteiro e traseiro dos dispositivos, consulte recursos dos painéis dianteiro e traseiro.

No painel traseiro de cada tipo de dispositivo, o conector serial e os conectores Ethernet podem ser gerenciados usando o Integrated Management Module. Para obter mais informações sobre o Integrated Management Module, consulte o *Guia do usuário do Integrated Management Module*.

3 Etapa 3: Pré-requisitos da instalação



Assegure-se de que os requisitos a seguir sejam atendidos:

- O hardware necessário esteja instalado.
- Para dispositivos QRadar, um notebook é conectado à porta serial na parte traseira do dispositivo ou um teclado e um monitor são conectados.
- Seu login esteja efetuado como usuário raiz.
- A chave de ativação esteja disponível.

Para garantir uma instalação bem-sucedida do IBM® Security QRadar® em seu dispositivo, deve-se instalar o sistema operacional Red Hat Enterprise Linux. Assegure-se de que seu dispositivo atenda aos requisitos do sistema para implementações do QRadar. Para obter mais informações, consulte o *QRadar Hardware Guide*.

4 Etapa 4: Instalando o QRadar SIEM em seu dispositivo



Observe que o QRadar Risk Manager e o QRadar Incident Forensics exigem licenças próprias e devem ser instalados em dispositivos separados. O QRadar Risk Manager deve ser instalado como um host gerenciado. O QRadar Vulnerability Manager pode ser instalado na mesma máquina que o console, em um console all-in-one.

1. Se estiver usando seu próprio dispositivo, monte a imagem ISO do QRadar.
 - a. Crie o diretório /media/cdrom digitando o comando a seguir:

```
mkdir /media/cdrom
```
 - b. Monte a imagem ISO do QRadar digitando comando a seguir:

```
mount -o loop <path to the QRadar ISO> /media/cdrom
```
 - c. Para iniciar a instalação, digite o comando a seguir:

```
/media/cdrom/setup
```
2. Quando for solicitada a chave de ativação, digite a sequência alfanumérica de 24 dígitos, com 4 partes, que você recebeu da IBM. A letra l e o número 1 (um) são equivalentes. A letra O e o número 0 (zero) também são equivalentes.
3. Para o tipo de instalação, selecione **Normal**.
4. Selecione o tipo de endereço IP.
5. No assistente, insira um nome completo do domínio, no campo **Nome do host**.
6. No campo **Endereço IP**, insira um endereço IP estático ou use o endereço IP atribuído pelo DHCP.
Para obter informações sobre como configurar um host primário ou secundário em IPv6, consulte *IBM Security QRadar High Availability Guide*.
7. Se você não tiver um servidor de email, insira localhost no campo **Nome do servidor de email**.
8. Clique em **Concluir**.
9. No campo **Senha raiz**, crie uma senha. As senhas devem ter no mínimo cinco caracteres, não devem conter espaços e podem conter os seguintes caracteres especiais: @, #, ^ e *.
10. Siga as instruções do assistente de instalação para concluir a instalação. O processo de instalação pode demorar vários minutos.

5 Etapa 5: Aplique a chave de licença



1. Efetue login no QRadar:

```
https://IP_Address_QRadar
```


O **Nome de usuário** padrão é administrador. A **Senha** é a senha da conta do usuário raiz.
2. Clique na guia **Administrador**.
3. Na área de janela de navegação, clique em **Configuração do sistema**.
4. Clique no ícone **Gerenciamento de sistema e de licença**.
5. Na caixa de listagem **Exibir**, selecione **Licenças** e faça upload da chave de licença.
6. Selecione a licença não alocada e clique em **Alocar sistema à licença**.
7. Na lista de licenças, selecione uma licença e clique em **Alocar licença ao sistema**.

6 Etapa 6: Introdução



Para obter mais informações introdutórias sobre como usar os componentes do QRadar, consulte os recursos a seguir.

- Introdução ao IBM Security QRadar SIEM
- Introdução ao IBM Security QRadar Risk Manager
- Introdução ao IBM Security QRadar Vulnerability Manager
- Introdução ao IBM Security QRadar Incident Forensics

Mais informações



Para obter a documentação integral do produto, visite o IBM QRadar Security Intelligence Platform Knowledge Center ou o Documento de Download.

