IBM QRadar Security Intelligence Platform

V7.2.6

快速入门指南

本指南使您初步了解典型安装。

本地语言版本: 要获取其他语言版本的《快速入门指南》，请从安装介质打印特定语言的 PDF。

产品概述

IBM® QRadar® Security Intelligence Platform 产品为集成安全信息和事件管理 (SIEM)、日志管理、异常检测、事件取证以及配置和漏洞管理提供了统一的体系结构。 本《快速入门指南》提供了关于安装 IBM Security QRadar 设备的信息。

1 步骤 1: 访问软件和文档

复审要安装的 QRadar 组件的发行说明。

从 IBM FIX Central Web 站点下载 QRadar 组件的 ISO。

2 步骤 2: 复审前面板和后面板功能

复审设备前面板和后面板功能的相关信息以确认连接和功能是否正确。

有关设备的前面板和后面板功能的更多信息，请参阅前面板和后面板功能。

在每个设备类型的后面板上，可使用集成管理模块来管理串行连接器和以太网连接器。有关集成管理模块的更多信息，请参阅 *Integrated Management Module User's Guide*。

3 步骤 3: 安装先决条件

确保满足以下需求:

- 已安装必需硬件。
- 对于 QRadar 设备，已将笔记本连接到设备后面的串口，或者已连接键盘和监视器。
- 以 root 用户身份登录。
- 提供了激活密钥。

要确保在您自己的设备上成功安装 IBM® Security QRadar®，您必须安装 Red Hat Enterprise Linux 操作系统。 确保设备满足 QRadar 部署的系统需求。 有关更多信息，请参阅 *QRadar Hardware Guide*。

4 步骤 4: 在您自己的设备上安装 QRadar SIEM

请注意，QRadar Risk Manager 和 QRadar Incident Forensics 需要其自己的许可证并必须安装在单独的设备上。 必须将 QRadar Risk Manager 安装为受管主机。 在一体化控制台中可以将 QRadar Vulnerability Manager 安装在与该控制台相同的机器上。

1. 如果要使用您自己的设备，请安装 QRadar ISO 映像:
   a. 通过输入以下命令来创建 /media/cdrom 目录:

      ```
      mkdir /media/cdrom
      ```

   b. 通过输入以下命令来安装 QRadar ISO 映像:

      ```
      mount -o loop <path to the QRadar ISO> /media/cdrom
      ```

   c. 要开始安装，请输入以下命令:

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

2. 当提示您输入激活密钥时，请输入 IBM 发给您的由 4 个部分组成的 24 位字母数字字符串。 字母 I 和数字 1（一）被视为相同字符。 字母 O 和数字 0（零）也被视为相同字符。
3. 对于设置类型，请选择**普通**。
4. 选择 IP 地址类型。
5. 在向导中的**主机名**字段中输入标准域名。
6. 在 **IP 地址**字段中，输入静态 IP 地址，或使用由 DHCP 分配的 IP 地址。

   有关设置 IPv6 主要主机或辅助主机的信息，请参阅 *IBM Security QRadar High Availability Guide*。
7. 如果您没有电子邮件服务器，请在**电子邮件服务器名称**字段中输入 `localhost`。
8. 单击**完成**。
9. 在 **root 用户密码**字段中，创建密码。密码至少必须为 5 个字符，不包含空格，可以包含以下特殊字符: @、#、^ 和 *。
10. 请遵循安装向导中的指示信息来完成安装。 安装流程可能会花费几分钟。

5 步骤 5: 应用许可证密钥

1. 登录 QRadar:

   ```
   https://IP_Address_QRadar
   ```

   缺省**用户名**为 `admin`。**密码** 为 root 用户帐户的密码。
2. 单击**管理**选项卡。
3. 在导航窗格中，单击**系统配置**。
4. 单击**系统和许可证管理**图标。
5. 从**显示**列表框中，选择**许可证**，然后上载许可证密钥。
6. 选择未分配的许可证，然后单击**将系统分配到许可证**。
7. 从许可证列表中，选择许可证，然后单击**将许可证分配到系统**。

6 步骤 6: 入门

有关使用 QRadar 组件入门的更多信息，请参阅以下资源:

- 初步了解 IBM Security QRadar SIEM
- 初步了解 IBM Security QRadar Risk Manager
- 初步了解 IBM Security QRadar Vulnerability Manager
- 初步了解 IBM Security QRadar Incident Forensics
- 初步了解IBM Security QRadar Packet Capture。

更多信息

要获取完整的产品文档，请访问 IBM QRadar Security Intelligence Platform Knowledge Center 或 下载文档。

部件号： CN6J5ML

Printed in Ireland