IBM QRadar Security Intelligence Platform

7.2.6 版

快速入門手冊

本手冊可讓您開始進行一般安裝。

國家語言版本：若要取得其他語言的《快速入門手冊》，請列印安裝媒體中的語言特定的 PDF。

產品概觀

IBM® QRadar® Security Intelligence Platform 產品提供一個統一的架構，用於整合安全資訊及事件管理 (SIEM)、日誌管理、異常偵測、事件辯論以及配置和漏洞管理。 此《快速入門手冊》提供安裝 IBM Security QRadar 軟體驅動裝置的相關資訊。

1 步驟 1： 存取軟體和說明文件

檢閱所要安裝之 QRadar 元件的版本注意事項。

從 the IBM FIX Central 網站下載 QRadar 元件的 ISO。

2 步驟 2： 檢閱前面板和後面板功能

檢閱軟體驅動裝置的前面板和後面板功能的相關資訊，以確認連線和功能正常。

如需軟體驅動裝置的前面板和後面板功能的相關資訊，請參閱前面板和後面板功能。

在每種軟體驅動裝置類型的後面板上，序列連接器及乙太網路連接器可使用「整合式管理模組」來管理。如需「整合式管理模組」的相關詳細資訊，請參閱 *Integrated Management Module User's Guide*（《整合式管理模組使用手冊》）。

3 步驟 3： 安裝必備項目

確保符合下列需求：

- 已安裝必要的硬體。
- 對於 QRadar 軟體驅動裝置，已將記事本連接至軟體驅動裝置背面的序列埠，或者已連接鍵盤和顯示器。
- 您已經以 root 使用者的身分登入。
- 有啓動鍵可用。

若要確保在您專屬的軟體驅動裝置上成功安裝 IBM® Security QRadar®，必須安裝 Red Hat Enterprise Linux 作業系統。請確保您的軟體驅動裝置符合 QRadar 部署的系統需求。 如需相關資訊，請參閱 *QRadar 硬體手冊*。

4 步驟 4： 在您專屬的軟體驅動裝置上安裝 QRadar SIEM

請注意，QRadar Risk Manager 及 QRadar Incident Forensics 需要各自的授權，並且必須安裝在個別軟體驅動裝置上。 QRadar Risk Manager 必須安裝爲受管理主機。 QRadar Vulnerability Manager 可安裝在一體式主控台中的主控台所在的相同機器上。

1. 如果您使用的是您專屬的軟體驅動裝置，請裝載 QRadar ISO 映像檔：
   a. 透過輸入下列指令，建立 /media/cdrom 目錄：

      ```
      mkdir /media/cdrom
      ```

   b. 透過輸入下列指令，裝載 QRadar ISO 映像檔：

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

   c. 若要開始安裝，請輸入下列指令：

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

2. 系統提示您輸入啓動鍵時，輸入 IBM 提供給您的分 4 個部分的 24 位英數字串。 字母 I 和數字 1（一）視爲相同。 字母 O 與數字 0（零）也視爲相同。
3. 對於安裝類型，選取**一般**。
4. 選取 IP 位址類型。
5. 在精靈中，在**主機名稱**欄位中輸入完整網域名稱。
6. 在 **IP 位址**欄位中，輸入靜態 IP 位址，或者使用 DHCP 分配的 IP 位址。

   如需設定 IPv6 主要或次要主機的相關資訊，請參閱*IBM Security QRadar 高可用性手冊*。
7. 如果您沒有電子郵件伺服器，請在**電子郵件伺服器名稱**欄位中輸入 `localhost`。
8. 按一下**完成**。
9. 在 **Root 密碼**欄位中，建立密碼。密碼至少必須包含 5 個字元，不得包含空格，可以包含下列特殊字元：@、#、^ 和 *。
10. 遵循安裝精靈中的指示完成安裝。 安裝過程可能需要數分鐘。

5 步驟 5： 套用授權金鑰

1. 登入 QRadar：

   ```
   https://IP_Address_QRadar
   ```

   預設**使用者名稱**是 `admin`。**密碼** 是 root 使用者帳戶的密碼。
2. 按一下**管理**標籤。
3. 在導覽窗格中，按一下**系統配置**。
4. 按一下**系統和授權管理**圖示。
5. 從**顯示**清單方框中，選取**授權**，然後上傳授權金鑰。
6. 選取未配置的授權，然後按一下**將系統配置給授權**。
7. 從授權清單中，選取授權，然後按一下**將授權配置給系統**。

6 步驟 6： 開始使用

如需開始使用 QRadar 元件的相關資訊，請參閱下列資源：

- 開始使用 IBM Security QRadar SIEM
- 開始使用 IBM Security QRadar Risk Manager
- 開始使用 IBM Security QRadar Vulnerability Manager
- 開始使用 IBM Security QRadar Incident Forensics
- 開始使用 IBM Security QRadar Packet Capture

其他資訊

如需完整的產品說明文件，請造訪 IBM QRadar Security Intelligence Platform Knowledge Center 或下載文件。

產品編號： CN6J5ML

Printed in Ireland