IBM Security QRadar Risk Manager

7.2.2 版

入門手冊

GI13-2710-00

附註

在使用本資訊及其所支援的產品之前，請閱讀第 27 頁的『聲明』中的資訊。

目錄

IBM Security QRadar Risk Manager 簡介

此資訊適用於 IBM® Security QRadar® Risk Manager。QRadar Risk Manager 是一種軟體驅動裝置，可用來監視裝置配置、模擬對網路環境的變更，以及設定網路中風險與漏洞的優先順序。

讀者對象

本手冊適用於負責在網路中安裝及配置 QRadar Risk Manager 系統的網路管理者。

技術說明文件

如需如何存取更多技術說明文件、技術文件及版本注意事項的相關資訊，請參閱存取 IBM Security Documentation 技術文件 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

與客戶支援中心聯絡

如需與客戶支援中心聯絡的相關資訊，請參閱支援與下載技術文件 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

良好安全實務聲明

IT 系統安全需要透過防護、偵測及回應來自企業內部與外部的不當存取，來保護系統及資訊。不當存取可能會導致資訊遭變更、損壞、不當使用或誤用，或者可能會導致系統遭損壞或誤用，其中包括用於對其他系統進行攻擊。沒有任何 IT 系統或產品應該視爲完全安全，也沒有任何單一產品、服務或安全方法可以完全有效地防止不當使用或存取。IBM 系統、產品及服務係設計爲全方位安全方法的一部分，因此必然將涉及其他作業程序，並且可能需要其他系統、產品或服務才能發揮最大效用。IBM 不保證任何系統、產品或服務免於或將讓貴企業免於任何一方的惡意或非法行爲。

第 1 章 開始使用 IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager 是個別安裝的軟體驅動裝置。使用 QRadar Risk Monitor 可監視裝置配置、模擬對網路環境的變更，以及設定網路中風險與漏洞的優先順序。

QRadar Risk Manager 是從 IBM Security QRadar SIEM 主控台上的**風險**標籤進行存取。

QRadar Risk Manager 透過向管理者提供工具來完成下列作業，從而加強 QRadar SIEM：

- 集中風險管理。
- 使用拓蹼來檢視網路。
- 配置及監視網路裝置。
- 檢視網路裝置之間的連線。
- 搜尋防火牆規則。
- 檢視現有規則及觸發規則的事件計數。
- 搜尋裝置及網路裝置的路徑。
- 監視及審核網路以確保相符性。
- 在網路上定義、排定及執行惡意探索模擬。
- 搜尋漏洞。

所增加資訊智慧的集中式風險管理及相符性，都可能涉及許多內部團隊的合作。作爲具有其他「風險管理」軟體驅動裝置的新一代 SIEM，我們會減少第一代 SIEM 產品所需要的步驟數。我們針對在 QRadar SIEM 中管理的資產，提供網路拓蹼及風險評量。

在評估處理程序期間，您可以透過聚集和相關性來合併系統、安全、風險分析及網路資訊，從而對網路環境提供完整的可見性。您還可以定義環境的入口網站，以提供無法使用手動處理程序及其他單點產品技術達到的可見性和有效性。

第 2 章 部署 IBM Security QRadar Risk Manager

QRadar Risk Manager 軟體驅動裝置會隨最新版本的 QRadar Risk Manager 軟體一起安裝。

您必須安裝 IBM Security QRadar Risk Manager 評估軟體驅動裝置。軟體需要啓動，且您必須將 IP 位址指派給 QRadar Risk Manager 軟體驅動裝置。

如果您需要啓動軟體及指派 IP 位址的協助，請與客戶支援中心聯絡。

軟體驅動裝置已備妥接受來自網路裝置的資訊。

如需使用 IBM Security QRadar Risk Manager 的相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

若要在環境中部署 QRadar Risk Manager，您必須：

1. 確保已安裝最新版本的 IBM Security QRadar SIEM。
2. 確保符合所有前置安裝需求。
3. 設定 QRadar Risk Manager 軟體驅動裝置，並開啓電源。
4. 在 QRadar SIEM 主控台上安裝 QRadar Risk Manager 外掛程式。
5. 在 QRadar SIEM 與 QRadar Risk Manager 軟體驅動裝置之間建立通訊。
6. 定義 QRadar Risk Manager 使用者的使用者角色。

安裝之前

您必須先完成 IBM Security QRadar SIEM 主控台的安裝處理程序，然後再安裝 IBM Security QRadar Risk Manager。最佳實務是在同一網路交換器上安裝 QRadar SIEM 和 QRadar Risk Manager。

您必須檢閱下列資訊：

- 配置防火牆埠存取權
- 識別網路設定
- QRadar Risk Manager 中不受支援的功能
- 受支援的 Web 瀏覽器

在安裝 IBM Security QRadar Risk Manager 評估軟體驅動裝置之前，請確保您具有：

- 兩個單元的軟體驅動裝置的空間
- 已裝載的框架滑軌與棚架

您可能想要選擇性地使用 USB 鍵盤及標準 VGA 監視器，來存取 QRadar SIEM 主控台。

配置防火牆上的埠存取

IBM Security QRadar SIEM 主控台與 IBM Security QRadar Risk Manager 之間的防火牆必須容許某些埠上的傳輸。

確保位於 QRadar SIEM 主控台與 QRadar Risk Manager 之間的任何防火牆都容許下列埠上的傳輸：

- 埠 443 (HTTPS)
- 埠 22 (SSH)
- 埠 37 UDP（時間）

識別網路設定

您必須在啓動安裝處理程序之前，收集網路設定的相關資訊。

收集網路設定的下列資訊：

- 主機名稱
- IP 位址
- 網路遮罩位址
- 子網路遮罩
- 預設閘道位址
- 主要「網域名稱系統 (DNS)」伺服器位址
- 次要 DNS 伺服器（選用）位址
- 使用「網址轉換 (NAT)」電子郵件伺服器名稱之網路的公用 IP 位址
- 電子郵件伺服器名稱
- 「網路時間通訊協定 (NTP)」伺服器（僅限主控台）或時間伺服器名稱

QRadar Risk Manager 中不受支援的功能

請務必注意 IBM Security QRadar Risk Manager 不支援的功能。

QRadar Risk Manager 中不支援下列功能：

- 高可用性 (HA)
- 「邊界閘道通訊協定 (BGP)」、「優先開放最短路徑 (OSPF)」或「路由資訊通訊協定 (RIP)」的動態遞送
- IPv6
- 非連續的網路遮罩
- 負載平衡的遞送
- 參照對映
- 儲存及轉遞

支援的 Web 瀏覽器

爲了 IBM Security QRadar 產品的功能正常運作，必須使用支援的 Web 瀏覽器。

存取 QRadar 系統時，會提示您輸入使用者名稱和密碼。使用者名稱和密碼必須由管理者事先進行配置。

下列表格列出了支援的 Web 瀏覽器版本。

表 1. QRadar 產品支援的 Web 瀏覽器

Web 瀏覽器	受支援的版本
Mozilla Firefox	17.0 延伸支援版 24.0 延伸支援版
32 位元 Microsoft Internet Explorer（已啓用文件模式及瀏覽器模式）	9.0
Google Chrome	自 IBM Security QRadar V7.2.2 產品發佈日期以來的最新版本

在 Internet Explorer 中啓用文件模式和瀏覽器模式

如果採用 Microsoft Internet Explorer 存取 IBM Security QRadar 產品，那麼必須啓用瀏覽器模式和文件模式。

程序

1. 在 Internet Explorer Web 瀏覽器中，按 F12 以開啓「開發者工具」視窗。
2. 按一下**瀏覽器模式**，並選取 Web 瀏覽器的版本。
3. 按一下**文件模式**。
   - 對於 Internet Explorer V9.0，選取 **Internet Explorer 9**
   - 對於 Internet Explorer V8.0，選取 **Internet Explorer 7.0 標準**

存取 IBM Security QRadar Risk Manager 使用者介面

IBM Security QRadar Risk Manager 使用 URL、使用者名稱及密碼的預設登入資訊。

您可以透過 QRadar SIEM 主控台存取 IBM Security QRadar Risk Manager。當您登入 IBM Security QRadar SIEM 主控台時，可使用下表中的資訊。

表 2. QRadar Risk Manager 的預設登入資訊

登入資訊	預設值
URL	https://<IP address>，其中 <IP address> 是 QRadar SIEM 主控台的 IP 位址。
使用者名稱	admin
密碼	安裝處理程序期間指派給 QRadar Risk Manager 的密碼。
授權金鑰	預設授權金鑰提供 5 週對系統的存取權。

設定 QRadar Risk Manager 軟體驅動裝置

您必須連接管理介面，並確保將電源連接線插入至 QRadar Risk Manager 軟體驅動裝置。

開始之前

閱讀、瞭解並取得必備項目。

關於這項作業

IBM Security QRadar Risk Manager 評估軟體驅動裝置是兩個單元的裝載式伺服器。評估設備並未提供框架滑軌與棚架。

QRadar Risk Manager 軟體驅動裝置包括四個網路介面。針對此評估，使用標示了 ETH0 的網路介面作爲管理介面。其他介面都是監視介面。所有介面都位於 QRadar Risk Manager 軟體驅動裝置的背板。

電源按鈕位於面板。

程序

1. 將管理網路介面連接至標示了 ETH0 的埠。
2. 確保專用電源連接線已插入至軟體驅動裝置背面。
3. 選用項目。若要存取 QRadar SIEM 主控台，請連接 USB 鍵盤與標準 VGA 監視器。
4. 如果軟體驅動裝置上有前嵌板，請拆除該嵌板，方法是推壓兩側的突起物，並將嵌板從軟體驅動裝置拉出。
5. 按下面板上的電源按鈕，以開啓軟體驅動裝置。

結果

軟體驅動裝置會開始開機處理程序。

將 QRadar Risk Manager 新增至 QRadar SIEM

您必須將 IBM Security QRadar Risk Manager 新增至 IBM Security QRadar SIEM，作爲受管理主機。

開始之前

如果您想要啓用壓縮，則每一個受管理主機的版本下限都必須是 QRadar SIEM 7.1 或 QRadar Risk Manager 7.1。

若要在「主控台」已 NAT 化時將非 NAT 化的受管理主機新增至部署，則必須將 QRadar SIEM 主控台變更爲已 NAT 化的主機。您必須先變更主控台，然後再將受管理的主機新增至部署。如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

程序

1. 開啓 Web 瀏覽器。
2. 鍵入 URL `https://<IP Address>`，其中 <IP Address> 是 QRadar SIEM 主控台的 IP 位址。
3. 鍵入您的使用者名稱及密碼。
4. 在**管理**標籤上，按一下**部署編輯器**。
5. 從功能表中選取**動作**，然後選取**新增受管理主機**。
6. 按**下一步**。
7. 輸入下列參數的值：

選項	敘述
輸入要新增之伺服器或軟體驅動裝置的 IP	QRadar Risk Manager 的 IP 位址。
輸入主機的 root 密碼	主機的 root 密碼。
確認主機的 root 密碼	確認密碼。
主機已 NAT 化	若要啓用受管理主機的 NAT，NAT 化網路必須使用靜態 NAT 轉換。如需相關資訊，請參閱 *IBM Security QRadarSIEM Administration Guide*。
啓用加密	建立主機的 SSH 加密通道。若要啓用兩個受管理主機之間的加密，每一個受管理主機都必須執行 QRadar SIEM 7.1 或 QRadar Risk Manager 7.1。
啓用壓縮	啓用兩個受管理主機之間的資料壓縮。

8. 選擇下列其中一個選項：
   - 如果您選取**主機已 NAT 化**勾選框，則必須輸入 NAT 參數的值。

選項	敘述
輸入要新增之伺服器或軟體驅動裝置的公用 IP	受管理主機的公用 IP 位址。受管理主機使用此 IP 位址，與使用 NAT 之不同網路中的其他受管理主機進行通訊。
選取已 NAT 化的網路	您希望此受管理主機使用的網路。 如果受管理主機與 QRadar SIEM 主控台位於同一子網路上，請選取已 NAT 化網路的主控台。 如果受管理主機與 QRadar SIEM 主控台並沒有位於同一子網路上，則選取已 NAT 化網路的受管理主機。

   - 如果您未選取**主機已 NAT 化**勾選框，請按**下一步**。
9. 按一下**完成**。 此處理程序可能要花費數分鐘才會完成。如果部署包括變更，則必須部署所有變更。
10. 按一下**部署**。

下一步

清除 Web 瀏覽器快取，然後登入 QRadar SIEM。現在，**風險**標籤已可使用。

建立通訊

您必須先在 QRadar Risk Manager 軟體驅動裝置與 QRadar SIEM 主控台之間建立通訊，然後再設定及配置 QRadar Risk Manager。

關於這項作業

建立通訊的處理程序可能要花費數分鐘才會完成。如果您要變更 QRadar Risk Manager 軟體驅動裝置的 IP 位址，或者需要將 QRadar Risk Manager 連接至另一個 QRadar SIEM 主控台，可以使用 QRadar SIEM **管理**標籤上的 **Risk Manager 設定**。

程序

1. 開啓 Web 瀏覽器，然後清除 Web 瀏覽器快取。
2. 登入 QRadar SIEM。如需 IP 位址、使用者名稱或 root 密碼的相關資訊，請參閱存取 IBM Security QRadar Risk Manager 使用者介面。
3. 按一下**風險**標籤。
4. 鍵入下列參數的值：

選項	敘述
IP/主機	QRadar Risk Manager 軟體驅動裝置的 IP 位址或主機名稱
Root 密碼	QRadar Risk Manager 軟體驅動裝置的 root 密碼。

5. 按一下**儲存**。

下一步

定義使用者角色。

新增 Risk Manager 使用者角色

您必須指派 Risk Manager 使用者角色，以提供對 QRadar Risk Manager 的存取權。

關於這項作業

依預設，QRadar SIEM 會提供預設管理角色，可提供對 QRadar Risk Manager 中所有項目的存取權。被指派管理專用權的使用者（其中包括預設管理角色）不能編輯他們自己的帳戶。另一個管理使用者必須進行任何必要變更。

如需建立及管理使用者角色的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表上，按一下**系統配置**。
3. 在**使用者管理**窗格中，按一下**使用者角色**。
4. 在左窗格中，選取您想要編輯的使用者角色。
5. 選取 **Risk Manager** 勾選框。
6. 按一下**儲存**。
7. 按一下**關閉**。
8. 在**管理**標籤上，按一下**部署變更**。

第 3 章 網路資料收集

您必須將 QRadar Risk Manager 配置爲從網路中的裝置讀取配置資訊。

從網路裝置收集的配置資訊會產生網路的拓蹼，並容許 QRadar Risk Manager 瞭解網路配置。

在 QRadar Risk Manager 中收集的資料，是用來在拓蹼中移入有關網路環境的主要資訊。

資料收集是含三個步驟的處理程序：

- 爲 QRadar Risk Manager 提供認證，以下載網路裝置配置。
- 探索裝置，以在「配置來源管理」中建立裝置清單。
- 備份裝置清單，以取得裝置配置，並在拓蹼中移入有關網路的資料。

認證

QRadar Risk Manager 必須配置認證，以存取及下載裝置配置。認證容許 QRadar Risk Manager 連接至防火牆、路由器、交換器或「入侵防護系統 (IPS)」裝置。

管理者使用**配置來源管理**來輸入裝置認證，這會向 QRadar Risk Manager 提供對特定裝置的存取權。QRadar Risk Manager 可以儲存特定網路裝置的個別裝置認證。如果多個網路裝置使用相同的認證，則您可以將認證指派給群組。例如，如果組織中的所有防火牆都具有相同的使用者名稱和密碼，則您可以將認證指派給群組。認證與所有防火牆的位址集相關聯，且可用來備份組織中所有防火牆的裝置配置。

註：如果特定裝置不需要網路認證，則**配置來源管理**中的參數可以保留空白。

配置認證

您可以配置網路裝置，爲 QRadar Risk Manager 提供對裝置的存取權。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表上，按一下**外掛程式**。
3. 在 **Risk Manager** 窗格上，按一下**配置來源管理**。
4. 在導覽功能表上，按一下**認證**。
5. 在**網路群組**窗格上，按一下**新增網路群組**。
6. 鍵入網路群組的名稱，並按一下**確定**。
7. 在**新增位址**欄位中，鍵入裝置的 IP 位址，並按一下**新增**。針對您必須新增的每一個位址重複此步驟。

   註：確保您新增的位址顯示在**新增位址**方框旁邊的「網路位址」區段中。請勿複製已存在於**配置來源管理**中其他網路群組內的裝置位址。
   您可以鍵入 IP 位址、IP 位址的範圍、CIDR 子網路或萬用字元。例如，若要使用萬用字元，請鍵入 10.1.*.*；或者若要使用 CIDR，請使用 10.2.1.0/24。

8. 在**認證**窗格上，按一下**新增認證集**。
9. 鍵入新認證集的名稱，並按一下**確定**。
10. 選取您建立之認證集的名稱，然後配置下列參數的值：

選項	敘述
使用者名稱	用來登入配接器的有效使用者名稱。 對於配接器，使用者名稱及密碼需要對數個檔案的存取權，例如 rule.C、objects.C、implied_rules.C 及 Standard.PF。
密碼	裝置的密碼。
啓用密碼	鍵入第二層次鑑別的密碼。 當認證提示「專家級模式」使用者認證時，需要此密碼。
SNMP 取得社群	選用項目
SNMPv3 鑑別使用者名稱	選用參數。
SNMPv3 鑑別密碼	選用參數。
SNMPv3 保密密碼	選用參數。 您想要用來解密 SNMPv3 設陷的通訊協定。

11. 按一下**確定**。

探索裝置

探索處理程序透過使用新增的認證，將網路裝置新增至拓蹼介面。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表上，按一下**外掛程式**。
3. 在 **Risk Manager** 區段中，按一下**配置來源管理**。
4. 在導覽功能表上，按一下**探索裝置**。
5. 鍵入 IP 位址或 CIDR 範圍，以指定您要探索的裝置位置。
6. 按一下**新增 (+)** 圖示。
7. 如果您要從已定義的 IP 位址或 CIDR 範圍中搜尋網路中的裝置，請選取**從上方定義的位址搜索網路**方框。
8. 按一下**執行**。

取得裝置配置

您可以備份裝置以下載裝置配置，從而 QRadar Risk Manager 可以在拓蹼中包括裝置資訊。

開始之前

您必須先配置認證集，然後才能下載裝置配置。

關於這項作業

您可以備份單一裝置或所有裝置。

如需從**工作**標籤排定自動化備份裝置配置的相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表上，按一下**外掛程式**。
3. 在 **Risk Manager** 窗格上，按一下**配置來源管理**。
4. 按一下**裝置**標籤。
5. 若要取得所有裝置的配置，請按一下導覽窗格中的**全部備份**。按一下**是**以繼續。
6. 若要取得特定裝置的配置，請選取個別裝置。若要選取備份多個裝置，請按住 Ctrl 鍵。按一下**備份**。

匯入裝置

使用「裝置匯入」，可利用逗點區隔值檔 (.CSV) 將配接器清單及其網路 IP 位址新增至「配置來源管理程式」。

裝置匯入清單最多可包含 5000 個裝置，但是清單必須針對匯入檔中的每一個配接器及其相關聯 IP 位址包含一行。

例如，

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

其中：

`<Adapter::Name>` 包含製造商及裝置名稱，例如，Cisco::IOS。

`<IP Address>` 包含裝置的 IP 位址，例如，191.168.1.1。

表 3. 裝置匯入範例

製造商	名稱	範例 <Adapter::Name>,<IP Address>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper 網路	Junos	Juniper::JUNOS,10.1.1.5

匯入 CSV 檔

您可以使用逗點區隔值 (CSV) 檔，將主要裝置清單匯入至「配置來源管理」。

開始之前

如果您匯入裝置清單，然後對 CSV 檔中的 IP 位址進行變更，則可能會意外地複製「配置來源管理」清單中的裝置。因此，請從「配置來源管理」中刪除裝置，然後重新匯入主要裝置清單。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表上，按一下**外掛程式**。
3. 在**外掛程式**窗格中，按一下**裝置匯入**。
4. 按一下**瀏覽**.
5. 找出 CSV 檔，按一下**開啓**。
6. 按一下**匯入裝置**。

結果

如果顯示錯誤，則您需要檢閱 CSV 檔來更正錯誤，並重新匯入該檔案。如果裝置清單結構不正確，或者如果裝置清單包含不正確的資訊，則匯入 CSV 檔可能會失敗。例如，CSV 檔可能遺漏冒號或指令，單一行上可能有多個裝置，或者配接器名稱有錯字。

如果裝置匯入中斷，則不會將 CSV 檔中的任何裝置新增至「配置來源管理」。

裝置匯入的疑難排解

如果您在嘗試匯入裝置之後收到錯誤訊息，可能是因爲匯入 CSV 檔失敗。

如果裝置清單結構不正確，則匯入裝置可能會失敗。例如，CSV 檔可能遺漏冒號或指令，或者多個裝置可能位於單一行上。

或者，如果裝置清單包含不正確的資訊，則匯入可能會失敗。例如，配接器名稱的拼字錯誤。

如果裝置匯入中斷，則不會將 CSV 檔中的任何裝置新增至「配置來源管理」。所安裝配接器的有效配接器名稱清單會顯示在訊息中。如果顯示錯誤，則必須檢閱 CSV 檔以更正任何錯誤。您可以在修正錯誤之後重新匯入檔案。

第 4 章 管理審核

IBM Security QRadar Risk Manager 透過協助您回答問題，有助於簡化評量網路安全原則及相符性需求。

相符性審核是安全管理者的必要、複雜作業。QRadar Risk Manager 會協助您回答下列問題：

- 如何配置我的網路裝置？
- 我的網路資源如何通訊？
- 我的網路漏洞在何處？

使用案例：配置審核

您可以使用由 QRadar Risk Manager 擷取的網路裝置配置資訊，以取得審核相符性並排定配置備份。

配置備份提供集中的自動方法，來記錄裝置變更，以取得審核相符性。配置備份會保存配置變更，並提供歷程參照；您可以擷取歷程記錄，或者針對另一個網路裝置比較配置。

QRadar Risk Manager 中的配置審核爲您提供下列選項：

- 網路裝置配置的歷程記錄。
- 正規化視圖，在您比較配置時顯示裝置變更。
- 用來搜尋裝置上規則的工具。

裝置的配置資訊是收集自「配置來源管理」中的裝置備份。每當 QRadar Risk Manager 備份裝置清單時，都會保存裝置配置的副本，以提供歷程參照。您排定「配置來源管理」的頻率越高，用於比較及歷程參照的配置記錄越多。

檢視裝置配置歷程

您可以檢視網路裝置的配置歷程。

關於這項作業

您可以檢視已備份之網路裝置的歷程資訊。此資訊可以從**配置監視器**頁面上的**歷程**窗格中進行存取。歷程窗格提供網路裝置配置的相關資訊，以及前次使用「配置來源管理」備份裝置配置的日期。

配置會顯示針對 QRadar Risk Manager 中網路裝置儲存的檔案類型。一般配置類型爲：

- **Standard-Element-Document** (SED)，是包含網路裝置相關資訊的 XML 資料檔。個別 SED 檔是以其原始 XML 格式檢視。如果 SED 與另一個 SED 檔相比較，則會正規化視圖，以顯示規則差異。
- **Config**，是由某些網路裝置提供的配置檔。這些檔案取決於裝置製造商。按兩下 config 檔，即可檢視配置檔。

註：根據您的裝置，可能會顯示數個其他配置檔。按兩下這些檔案會以純文字格式顯示內容。純文字視圖支援 Web 瀏覽器視窗中的尋找 (Ctrl+F)、貼上 (Ctrl+V) 及複製 (Ctrl+C) 功能。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，按一下**配置監視器**。
3. 按兩下配置以檢視詳細的裝置資訊。
4. 按一下**歷程**。
5. 在**歷程**窗格上，選取配置。
6. 按一下**檢視選取項目**。

比較單一裝置的裝置配置

您可以比較單一裝置的裝置配置。

關於這項作業

如果您比較的檔案是 Standard-Element-Document (SED)，則可以檢視配置檔之間的規則差異。

當您比較正規化配置時，文字的顏色指出下列規則：

- 綠色點虛線外框指出已新增至裝置的規則或配置。
- 紅色虛線外框指出已從裝置刪除的規則或配置。
- 黃色實線外框指出已在裝置上修改的規則或配置。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，按一下**配置監視器**。
3. 按兩下任何裝置以檢視詳細配置資訊。
4. 按一下**歷程**以檢視此裝置的歷程。
5. 選取主要配置。
6. 按下 Ctrl 鍵，並選取第二個配置以進行比較。
7. 在**歷程**窗格上，按一下**比較選取項目**。
8. 選用項目。若要檢視原始配置差異，請按一下**檢視原始比較**。 如果是針對配置檔或另一個備份類型進行比較，則會顯示原始比較。

比較不同裝置的裝置配置

您可以比較不同裝置的兩個配置。

關於這項作業

如果您比較的檔案是 Standard-Element-Document (SED)，則可以檢視配置檔之間的規則差異。

當您比較正規化配置時，文字的顏色指出下列規則：

- 綠色點虛線外框指出已新增至裝置的規則或配置。

- 紅色虛線外框指出已從裝置刪除的規則或配置。
- 黃色實線外框指出已在裝置上修改規則或配置。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，按一下**配置監視器**。
3. 按兩下任何裝置以檢視詳細配置資訊。
4. 按一下**歷程**以檢視此裝置的歷程。
5. 選取主要配置。
6. 按一下**標示要比較**。
7. 從導覽功能表中，選取**所有裝置**以回到裝置清單。
8. 按兩下要比較的裝置，並按一下**歷程**。
9. 選取另一個配置備份，以與所標示的配置進行比較。
10. 按一下**與標示項目進行比較**。
11. 選用項目。若要檢視原始配置差異，請按一下**檢視原始比較**。 如果比較用於配置檔或另一個備份類型，則會顯示原始比較。

使用案例：檢視拓蹼中的網路路徑

QRadar Risk Manager 中的拓蹼以圖形表示法顯示網路裝置。

拓蹼路徑搜尋可以判定網路裝置如何進行通訊，以及它們用來通訊的網路路徑。路徑搜尋容許 QRadar Risk Manager 以視覺化方式顯示來源與目的地之間的路徑，以及埠、通訊協定及規則。

您可以檢視裝置如何進行通訊，這對受安全保護或受限的存取資產非常重要。

主要功能包括：

- 檢視網路上裝置之間通訊的能力。
- 使用過濾器來搜尋拓蹼中的網路裝置。
- 快速存取以檢視裝置規則及配置。
- 檢視自路徑搜尋產生之事件的能力。

搜尋拓蹼

您可以透過搜尋拓蹼來檢視裝置通訊。

關於這項作業

路徑搜尋是用來過濾拓蹼模型。路徑搜尋包括所有包含來源 IP 位址或 CIDR 範圍的網路子網路、包含目的地 IP 位址或 CIDR 範圍的子網路（也容許其使用所配置通訊協定及埠進行通訊）。該搜尋會檢查現有拓蹼模型，並包括來源與目的地之間通訊路徑中涉及的裝置，以及詳細連線資訊。

如果您的拓蹼包括「入侵防護系統 (IPS)」，則可以使用漏洞來過濾搜尋。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，按一下**拓蹼**。
3. 從**搜尋**清單框中，選取**新搜尋**。
4. 在**搜尋準則**窗格中，選取**路徑**。
5. 在**來源 IP/CIDR** 欄位中，鍵入您要過濾拓蹼模型所在的 IP 位址或 CIDR 範圍。請使用逗點來分隔多個項目。
6. 在**目的地 IP/CIDR** 欄位中，鍵入您要過濾拓蹼模型所在的目的地 IP 位址或 CIDR 範圍。請使用逗點來分隔多個項目。
7. 選用項目。從**通訊協定**清單中，選取您要用來過濾拓蹼模型的通訊協定。
8. 選用項目。在**目的地埠**欄位中，鍵入您要過濾拓蹼模型所在的目的地埠。請使用逗點來分隔多個埠。
9. 按一下**確定**。
10. 將滑鼠移至連接線上方，以檢視連線的相關詳細資料。 如果搜尋連接至包含規則的裝置，則裝置規則鏈結會顯示在對話框中。

使用案例：視覺化攻擊的攻擊路徑

QRadar Risk Manager 中的攻擊是系統產生的事件，用來向您警示網路狀況或事件。

攻擊路徑視覺化會將攻擊與拓蹼搜尋連結在一起。這個視覺化容許安全操作員檢視攻擊詳細資料，以及攻擊透過網路採用的路徑。攻擊路徑會爲您提供視覺化表示法。視覺化表示法可顯示網路中進行通訊以容許攻擊透過網路傳輸的資產。此資料在審核期間很重要，可證明對攻擊進行監視，也可證明攻擊在網路中沒有替代路徑通往重要資產。

視覺化的主要功能爲：

- 利用 QRadar SIEM 的現有規則及攻擊系統。
- 顯示攻擊來源與目的地之間所有裝置的視覺化路徑。
- 快速存取容許攻擊的裝置配置及規則。

監視攻擊的攻擊路徑

您可以檢視攻擊的攻擊路徑。攻擊路徑會顯示來源、目的地及相關聯的裝置。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**所有攻擊**。 **所有攻擊**頁面即會顯示您網路上的攻擊清單。系統會從最高強度開始列出攻擊。
3. 按兩下攻擊以開啓攻擊摘要。
4. 在**攻擊**工具列上，按一下**檢視攻擊路徑**。

第 5 章 使用案例：監視原則

原則審核與變更控制是基本處理程序，容許管理者與安全專家控制重要商業資產之間的存取與通訊。

原則監視準則可以包括對下列實務範例的資產及通訊的監視：

- 我的網路包含針對 PCI 第 1 部分審核具有風險配置的資產嗎？
- 我的資產容許使用 PCI 第 10 部分審核的有風險通訊協定進行通訊嗎？
- 我如何瞭解原則變更何時讓我的網路違規？
- 我如何檢視穩定或高風險資產的漏洞？
- 我如何檢視含漏洞與網際網路存取之網路中的資產？

使用「原則監視器」，以定義基於風險指示器的測試，然後限制測試結果來過濾查詢，以取得特定結果、違規、通訊協定或漏洞。

IBM Security QRadar Risk Manager 包括數個依 PCI 種類分組的「原則監視器」問題。例如，PCI 1、PCI 6 及 PCI 10 問題。可以針對資產或裝置及規則建立問題，以公開網路安全風險。將有關資產或裝置/規則的問題提交至「原則監視器」之後，傳回的結果會指定風險層次。您可以核准從資產傳回的結果，或者定義希望系統如何回應未核准的結果。

「原則監視器」提供下列主要功能：

- 預先定義的「原則監視器」問題，以協助工作流程。
- 判定使用者是否使用了禁止的通訊協定進行通訊。
- 評量特定網路上的使用者是否能夠與禁止的網路或資產進行通訊。
- 評量防火牆規則是否符合公司原則。
- 連續監視向管理者產生攻擊或警示的原則。
- 透過評量哪些系統可能由於裝置配置而受損，來設定漏洞的優先順序。
- 協助識別相符性問題。

使用案例：評量具有可疑配置的資產

組織使用公司安全原則，來定義風險以及資產與網路之間容許的通訊。爲了在相符性及公司原則的違反方面提供協助，組織會使用「原則監視器」來評量及監視可能不明的風險。

PCI 相符性要求您識別包含持卡人資料的裝置，然後繪圖、驗證通訊並監視防火牆配置，以保護包含機密資料的資產。「原則監視器」會提供方法，可讓您快速符合這些需求，並可讓管理者遵從公司原則。減少風險的一般方法，包括識別並監視與未受保護通訊協定進行通訊的資產。這些通訊協定（例如，路由器、防火牆或交換器）容許 FTP 或 Telnet 連線。使用「原則監視器」，可識別拓蹼中配置有風險的資產。

PCI 第 1 部分的問題可能包括下列準則：

- 容許已禁止通訊協定的資產。
- 容許有風險通訊協定的資產。

- 容許跨網路之不符合原則應用程式的資產。
- 容許網路（其包含受保護的資產）中不符合原則應用程式的資產。

評量容許有風險通訊協定的裝置

使用「原則監視器」來評量容許有風險通訊協定的裝置。

關於這項作業

QRadar Risk Manager 會評估問題，並顯示拓蹼中任何符合測試問題的資產結果。您網路中的安全專家、管理者或審核員，可以核准與特定資產的無風險通訊。他們還可以針對行爲建立攻擊。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表中，按一下**原則監視器**。
3. 從「群組」清單框中，選取 **PCI 1**。
4. 選取測試問題**評量從網際網路到 DMZ 中任何容許有風險通訊協定（即 Telnet 與 FTP 傳輸 - 分別是埠 21 與 23）的裝置（即防火牆）**。
5. 按一下**提交問題**。

使用案例：評量具有可疑通訊的資產

使用「原則監視器」，可透過追蹤、記載及顯示網路資產的存取，來識別 PCI 第 10 部分相符性。

QRadar Risk Manager 可透過識別拓蹼中容許可疑或有風險通訊的資產，來協助識別 PCI 第 10 部分相符性。QRadar Risk Manager 可以檢查這些資產中是否有實際通訊或可能的通訊。實際通訊會顯示已使用問題準則進行通訊的資產。可能的通訊會顯示可使用問題準則進行通訊的資產。

PCI 第 10 部分問題可以包括下列準則：

- 容許將問題送入內部網路的資產。
- 從未授信位置與授信位置進行通訊的資產。
- 從 VPN 與授信位置進行通訊的資產。
- 容許授信位置內未加密之不符合原則通訊協定的資產。

尋找容許通訊的資產

您可以尋找容許從網際網路進行通訊的資產。

關於這項作業

QRadar Risk Manager 會評估問題，並顯示容許來自網際網路之入埠連線的任何內部資產結果。您網路中的安全專家、管理者或審核員，可以核准與不被視爲安全或包含客戶資料的資產進行通訊。隨著所產生事件的增多，您可以在 QRadar SIEM 中建立攻擊，以監視此類型的有風險通訊。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表中，按一下**原則監視器**。
3. 從「群組」清單框中，選取 **PCI 10**。
4. 選取測試問題**評量從網際網路到內部網路任何位置的任何入埠連線**。
5. 按一下**提交問題**。

使用案例：監視原則違規

QRadar Risk Manager 可以持續監視「原則監視器」中任何預先定義或使用者產生的問題。您可以使用監視模式，以在 QRadar Risk Manager 中產生事件。

當您選取要監視的問題時，QRadar Risk Manager 會每小時針對您的拓蹼分析問題，以判定資產或規則變更是否產生未核准的結果。如果 QRadar Risk Manager 偵測到未核准的結果，則可以產生攻擊，以警示您有關所定義原則中的偏差。在監視模式下，QRadar Risk Manager 可以同步監視 10 個問題的結果。

問題監視提供下列主要功能：

- 每小時監視規則或資產變更是否有未核准的結果。
- 使用高階及低階事件種類，將未核准的結果分類。
- 對未核准的結果產生攻擊、電子郵件、syslog 訊息或儀表板通知。
- 在 QRadar SIEM 中使用事件檢視、相關性、事件報告、自訂規則及儀表板。

配置問題

您可以使用「原則監視器」來配置要監視的問題。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表中，按一下**原則監視器**。
3. 選取您要監視的問題。
4. 按一下**監視器**。
5. 配置監視問題所需要的任何選項。
6. 按一下**儲存監視器**。

結果

即會針對問題啓用監視，並根據監視準則產生事件或攻擊。

使用案例：使用漏洞來設定風險的優先順序

已公開的漏洞是網路資產的重要風險因數。

QRadar Risk Manager 會利用「原則監視器」中的資產資訊及漏洞資訊。此資訊是用來判定資產是否易受輸入類型攻擊，例如，SQL 注入、隱藏的欄位及點閱綁架。

在資產上偵測到的漏洞，可依網路位置或有漏洞的另一個裝置的連線，設定優先順序。

漏洞資產問題可以包括下列準則：

- 具有特定日期之後報告的新漏洞的資產。
- 具有特定漏洞或 CVSS 評分的資產。
- 具有特定漏洞分類（例如，輸入操縱、阻斷服務或已驗證的 OSVDB）的資產。

尋找有漏洞的資產

您可以尋找有漏洞的資產。

關於這項作業

QRadar Risk Manager 會評估問題，並顯示包含漏洞的資產結果。安全專家、管理者或審核員可以識別網路中包含已知 SQL 注入漏洞的資產。他們可以快速修補連接至受保護網路的任何資產。隨著所產生事件的增多，您可以在 QRadar SIEM 中建立事件或攻擊，以監視包含 SQL 注入漏洞的資產。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表中，按一下**原則監視器**。
3. 從**群組**清單中，選取**漏洞**。
4. 選取測試問題**評量特定本端網路（即受保護的伺服器網路）上具有 SQL 注入漏洞的資產**。
5. 按一下**提交問題**。

使用案例：依區域或網路通訊設定資產漏洞的優先順序

漏洞與受保護資產位於同一網路中的系統具有資料流失的高度風險。

依區域或網路偵測資產上的漏洞，是在網路中發生惡意探索之前予以防止的主要方法。PCI 第 6.1 與 6.2 部分規定您要在漏洞修補程式發行的一個月之內檢閱並修補系統。QRadar Risk Manager 會協助自動化修補處理程序，並設定優先順序。在資產上偵測到漏洞之後，可依網路位置或有漏洞的另一個裝置的連線，設定優先順序。對於可連接至可疑區域的安全網路，或是其 CVSS 評分高於內部原則容許的資產，設定優先順序非常重要。

有漏洞的資產問題可以包括下列準則：

- 具有用戶端漏洞的資產（與可疑地理區域進行通訊且包含受保護資產）。
- 特定網路中具有阻斷服務漏洞的資產。
- 特定網路中具有郵件漏洞的資產。
- 具有漏洞及特定「通用漏洞評分系統 (CVSS)」評分的資產。

尋找網路中有漏洞的資產

您可以尋找特定網路中有漏洞的資產。

關於這項作業

QRadar Risk Manager 會評估問題，並顯示包含作業系統特定漏洞之特定位置中的結果。您網路的安全專家、管理者或審核員，可以核准與不被視爲安全或包含客戶資料的資

產進行通訊。隨著所產生事件的增多，您可以建立攻擊，以監視此類型的有風險通訊。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表中，按一下**原則監視器**。
3. 從**群組**清單框中，選取**漏洞**。
4. 選取測試問題**評量特定本端網路上具有作業系統特定漏洞的資產**。
5. 按一下**提交問題**。

第 6 章 模擬的使用案例

使用案例：模擬網路資產上的攻擊

您可以使用模擬，來測試各種來源的網路漏洞。

您可以使用攻擊模擬，來審核網路中的裝置配置。

模擬提供下列主要功能：

- 模擬顯示可能會對網路採取攻擊的推理路徑排列。
- 模擬顯示攻擊如何能透過網路裝置傳播以擴展至其他資產。
- 模擬容許監視以偵測新的曝光網站。

建立模擬

您可以在 SSH 通訊協定上建立網路攻擊的模擬。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，選取**模擬 > 模擬**。
3. 從**動作**清單中，選取**新建**。
4. 鍵入模擬的名稱。
5. 選取**現行拓蹼**。
6. 選取**使用連線資料**勾選框。
7. 從**您想要從何處開始模擬**清單中，選取模擬的原點。
8. 新增模擬攻擊**攻擊使用通訊協定將下列其中一個開啓的埠作為目標**。
9. 針對此模擬中，按一下**開啓埠**，然後新增埠 22。
10. 按一下**通訊協定**，然後選取 **TCP**。 SSH 使用 TCP。
11. 按一下**確定**。
12. 按一下**儲存模擬**。
13. 從**動作**清單中，選取**執行模擬**。 結果直欄包含一個清單，內有模擬的執行日期以及檢視結果的鏈結。
14. 按一下**檢視結果**。

結果

即會在結果中顯示包含 SSH 漏洞的資產清單，容許網路管理者核准網路中容許或預期的 SSH 連線。可以針對事件或攻擊監視未核准的通訊。

所顯示的結果會以視覺化表示法，爲您的網路管理者或安全專家，提供攻擊在網路中可能採用的攻擊路徑及連線。例如，第一步提供受模擬影響的直接連接的資產清單。第二步列出網路中可以與模擬中第一層資產進行通訊的資產。

攻擊中提供的資訊，可讓您針對數以千計的可能攻擊實務範例，來強化並測試網路。

使用案例：模擬網路配置變更的風險

您可以使用拓蹼模型，來根據現有網路定義虛擬網路模型。您可以根據可結合並配置的一系列修改，建立網路模型。

您可以使用拓蹼模型，利用模擬來判定網路上配置變更的效果。

拓蹼模型提供下列主要功能：

- 建立測試網路變更的虛擬拓蹼。
- 模擬針對虛擬網路的攻擊。
- 透過測試降低受保護資產的風險與曝光。
- 虛擬網路區段可讓您隔離並測試網路或資產的機密部分。

若要模擬網路配置變更：

1. 建立拓蹼模型。
2. 模擬針對拓蹼模型的攻擊。

建立拓蹼模型

您可以建立拓蹼模型，以測試網路變更及模擬攻擊。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，選取**模擬 > 拓蹼模型**。
3. 從**動作**清單中，選取**新建**。
4. 鍵入模型的名稱。
5. 選取您要套用至拓蹼的任何修改。
6. 配置已新增至**依下列方式配置模型**窗格的測試。
7. 按一下**儲存模型**。

下一步

爲您的新拓蹼模型建立模擬。

模擬攻擊

您可以在埠及通訊協定上模擬攻擊。

程序

1. 按一下**風險**標籤。
2. 在導覽功能表上，選取**模擬 > 模擬**。
3. 從**動作**清單框中，選取**新建**。
4. 鍵入模擬的名稱。
5. 選取您建立的拓蹼模型。
6. 從**您想要從何處開始模擬**清單中，選取模擬的原點。
7. 新增模擬攻擊**攻擊使用通訊協定將下列其中一個開啓的埠作為目標**。
8. 針對此模擬，按一下**開啓埠**，然後新增埠 22。

9. 按一下**通訊協定**，然後選取 TCP。 SSH 使用 TCP。
10. 按一下**確定**。
11. 按一下**儲存模擬**。
12. 從**動作**清單中，選取**執行模擬**。 結果直欄包含一個清單框，內有模擬的執行日期以及檢視結果的鏈結。
13. 按一下**檢視結果**。

聲明

本資訊係針對 IBM 在美國所提供之產品與服務所開發。

在其他國家或地區中，IBM 不見得有提供本文件所提及之各項產品、服務或功能。 請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。 這份文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 產品、程式或服務。只要未侵犯 IBM 之智慧財產權，任何功能相當之產品、程式或服務皆可取代 IBM 之產品、程式或服務。不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

本文件所說明之主題內容，IBM 可能擁有其專利或專利申請案。 提供本文件不代表授予這些專利的授權。 您可以書面提出授權查詢，來函請寄到：

IBM Director of Licensing
IBM CorporationNorth Castle Drive
Armonk, NY 10504-1785 U.S.A.

如果是有關雙位元組字集 (DBCS) 資訊的授權查詢，請洽詢所在國的 IBM 智慧財產部門，或書面提出授權查詢，來函請寄到：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

下段對英國或任何對這些規定與當地法律不一致的其他國家或地區不適用：

IBM 僅以「現狀」提供本書，而不提供任何明示或默示之保證 (包括但不限於可售性或符合特定效用的保證)。有些地區在特定交易上，不允許排除明示或暗示的保證，因此，這項聲明不一定適合您。

本資訊中可能會有技術上或排版印刷上的訛誤。 因此，IBM 會定期修訂；並將修訂後的內容納入新版中。 IBM 隨時會改進及/或變更本出版品所提及的產品及/或程式，不另行通知。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供保證。 這些網站中的教材不屬於此 IBM 產品的相關教材，用戶使用這些網站時應自行承擔風險。

IBM 得以各種 IBM 認爲適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。

如果本程式之獲授權人爲了 (i) 在個別建立的程式和其他程式（包括本程式）之間交換資訊，以及 (ii) 相互使用所交換的資訊，因而需要相關的資訊，請洽詢：

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

這些資訊可依適當條款而取得，在某些情況下必須付費方得使用。

IBM 基於 IBM 客戶合約、IBM 國際程式授權合約或雙方之任何同等合約的條款，提供本文件所提及的授權程式與其所有適用的授權資料。

本文件中所含的任何效能資料是在控制環境中得出。因此，在其他作業環境中獲得的結果可能有明顯的差異。在開發層次的系統上可能有做過一些測量，但不保證這些測量在市面上普遍發行的系統上有相同的結果。再者，有些測定可能是透過推測方式來評估。實際結果可能不同。本文件的使用者應驗證其特定環境適用的資料。

本書所提及之非 IBM 產品資訊，取自產品的供應商，或其發佈的聲明或其他公開管道。IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性或任何對產品的其他主張是否完全無誤。 有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

有關 IBM 未來動向的任何陳述，僅代表 IBM 的目標和目的而已，並可能於未事先聲明的情況下有所變動或撤回。

所有 IBM 價格爲 IBM 之建議零售價，可隨時更改而不另行通知。經銷商之價格可與此不同。

本資訊含有日常業務運作所用的資料和報告範例。爲求儘可能地完整說明，範例包括了個人、公司、品牌和產品的名稱。所有這些名稱都是虛構的，如有任何類似實際企業所用的名稱及地址之處，純屬巧合。

若貴客戶正在閱讀本項資訊的電子檔，可能不會有照片和彩色說明。

商標

IBM、IBM 標誌及 ibm.com® 是 International Business Machines Corporation 在美國及/或其他國家或地區的商標或註冊商標。如果這些和其他 IBM 商標術語在本資訊中第一次出現時以商標符號（® 或 ™）標示，則這些符號指出發佈本資訊時，IBM 擁有美國註冊或一般法律商標。此類商標也可能是其他國家或地區的註冊或一般法律商標。IBM 商標的最新清單可在 Web 的 Copyright and trademark information (www.ibm.com/legal/copytrade.shtml) 中找到。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其他國家或地區的商標。

其他公司、產品及服務名稱可能是其他公司的商標或服務標記。

隱私權條款考量

IBM 軟體產品（包括作爲服務解決方案的軟體，即「軟體產品與服務」）可能使用 Cookie 或其他技術來收集產品使用資訊，以有助於改善一般使用者體驗、自訂與一般使用者的互動或爲了其他目的。在許多情況下，「軟體供應項目」不會收集任何個人識別資訊。我們的部分「軟體供應項目」有助於讓您能收集個人識別資訊。如果此「軟體供應項目」使用 Cookie 來收集個人識別資訊，則以下提出此供應項目使用 Cookie 的相關資訊。

視部署的配置而定，「軟體產品與服務」可能使用階段作業 Cookie 收集每個使用者的階段作業 ID，用於階段作業管理和鑑別。這些 Cookie 可以停用，但是這也將刪除它們啓用的功能。

如果爲此「軟體供應項目」部署的配置讓您的客戶能夠透過 Cookie 及其他技術，從一般使用者收集個人識別資訊，則應該探查適用於此類資料收集之任何法律的您自己的合法建議，其中包括通知及同意的任何需求。

如需針對這些目的的各種技術（其中包括 Cookie）的使用的相關資訊，請參閱 Cookies, Web Beacons and Other Technologies 中的 IBM 的隱私權原則（網址爲 http://www.ibm.com/privacy ），以及 IBM 的線上隱私權條款（網址爲 http://www.ibm.com/privacy/details），以及「IBM 軟體產品及軟體作爲服務隱私權條款」（網址爲 http://www.ibm.com/software/info/product-privacy）。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

N

P

R

S

W