IBM Security QRadar

Master Console

0.11.0 版

附註

在使用本資訊及其所支援的產品之前，請閱讀第 17 頁的『聲明』中的資訊。

目錄

Master Console 簡介

IBM® Security QRadar® 管理者使用 Master Console 來檢視部署與主機的性能及其他相關資訊。

讀者對象

本手冊面向負責調查及管理網路安全的所有 QRadar 使用者。 若要使用此資訊，您必須具有 QRadar 存取權並瞭解公司網路與連網技術。

技術文件

若要在 Web 上尋找 IBM Security QRadar 產品說明文件，包括所有翻譯文件，請存取 IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)。

如需如何在 QRadar 產品檔案庫中存取更多技術文件的相關資訊，請參閱存取 IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

聯絡客戶支援中心

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

良好安全實務的陳述

IT 系統安全涉及透過預防、偵測及回應企業內外的不當存取來保護系統與資訊。不當存取可能導致變更、損壞、不當或誤用資訊，也可能導致損壞或誤用系統，包括用於攻擊其他系統。 沒有任何 IT 系統或產品應該被看作完全安全，且沒有單個產品、服務或安全手段可以完全有效預防不當使用或存取。 IBM 系統、產品及服務係設計為合法的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為。

請注意：

使用本程式可能會與部分法律或法規相抵觸，包括那些與隱私權、資料保護、僱佣及電子通訊與儲存相關的法律或法規。IBM Security QRadar 必須以合法之目的並透過合法方式使用。 客戶同意在遵循適用法律、法規及原則，並承擔所有責任的前提下使用本程式。 被授權方代表它將取得或已取得合法使用 IBM Security QRadar 所需的同意、許可權或授權。

Master Console

使用 Master Console 來監視 IBM Security QRadar 部署。

Master Console 在 Managed Security Service Providers (MSSP) 環境中很有用。使用儀表板，您可以同時監視多個部署。

透過諸如 CPU 使用率、網路與磁碟活動、記憶體用量以及事件與流程速率等作業資料的視覺化表示法，您可以輕鬆監視部署的性能。

集中化攻擊管理視圖會依長度順序顯示所有部署中的攻擊。您可以往下探查資訊，然後登入特定的 QRadar 部署，以取得攻擊的相關資訊。

Master Console 中管理者的新增功能

瞭解每一個 Master Console 發行版中的新增特性。

Master Console 0.11.0 版中的新增功能

Master Console 0.11.0 版包含下列安裝及設計變更：

安裝

當您安裝 QRadar 7.2.8 版 時會安裝 Master Console 0.11.0 版。您無法獨立下載該產品。

導覽改進項目

新的浮動功能表使用單字代替圖示，使導覽更為直觀且便於您尋找要查看的頁面。

Master Console 0.10.0 版中的新增功能

Master Console 0.10.0 版引進了承租人與網域狀態提示、搜尋及過濾使用者清單的功能以及在未來升級中保留基於範圍的資訊等功能。

搜尋及過濾 Master Console 使用者

使用新搜尋列，您可以建置文字及欄位型查詢，以過濾**使用者管理**視窗上顯示的 Master Console 使用者清單。

進一步瞭解如何過濾 Master Console 使用者清單...

承租人與網域狀態提示

Master Console 現在可顯示針對您監視之每一個部署所配置的承租人與網域的相關資訊。按一下**受管理主機**頁面上的**承租人**標籤可檢視每一個承租人的事件及流程比率限制。

進一步瞭解如何檢視 QRadar 部署的相關資訊...

改進了範圍資訊在未來升級中的處理方式

配置第三方鑑別提供者之後，Master Console 未來升級將保留範圍設定。若要利用此改進，您必須在升級至 Master Console 0.10.0 版或在第一次配置第三方鑑別提供者時，將範圍資訊新增至 `shiro.realms` 檔案。

 進一步瞭解如何配置鑑別提供者...

使用 YUM 套件管理程式安裝 Master Console

現在使用 Yellowdog Updater Modified (YUM) 指令來安裝 Master Console，該指令可提供改進的相依關係檢查及套件管理功能。

 進一步瞭解如何安裝 Master Console...

改進了資料驗證及訊息

新增部署、**編輯部署**及**使用者管理**視窗進行了重新設計，可在您管理部署及使用者帳戶時提供改良的資料驗證及參考訊息。

Master Console 0.9.1 版中的新增功能

Master Console 0.9.1 版併入了更新項目以修正「部署」更新頻率，以及確保 Master Console 可以與 IBM Security QRadar 的更新版本搭配使用。

Master Console 0.9.0 版中的新增功能

Master Console 0.9.0 版中引進了搜尋及過濾攻擊的功能，並移除了對 Microsoft Internet Explorer 10 的支援。

搜尋及過濾攻擊

使用新搜尋列，您可以建置文字及欄位型查詢，以過濾合併攻擊清單上顯示的攻擊。

 進一步瞭解...

更新支援的瀏覽器

本發行版中捨棄了對 Microsoft Internet Explorer 10 瀏覽器的支援。  進一步瞭解...

Master Console 0.8.1 版中的新增功能

Master Console 0.8.1 版中引進了對 Active Directory 及 LDAP 安全提供者的本端使用者管理及支援。

使用者管理

您可以將本端使用者的存取權授與 Master Console 並進行控制。升級至 Master Console 0.8.1 版或更新版本之後，所有現有 QRadar 使用者都會以本端使用者身分移轉至 Master Console。您在 Master Console 中管理使用者，包括新增使用者及變更密碼。

 進一步瞭解...。

安全提供者整合

您可以使用現有的 Active Directory 或 LDAP 安全基礎架構，以配置使用者鑑別。

 進一步瞭解...

Master Console 入門

安裝 Master Console 以監視 IBM Security QRadar 部署中的所有 QRadar 主機的性能及系統。

支援的環境

安裝及使用 Master Console 之前，請驗證環境中具有支援的軟硬體。

硬體需求

Master Console 在 QRadar 3105 軟體驅動裝置上執行。

安裝 Master Console 之前，請確認虛擬或實體軟體驅動裝置符合下列硬體規格：

表 *1. QRadar 3105* 軟體驅動裝置概觀

說明	值
處理器	8
介面	兩個 10/100/1000 Base-T 網路監視介面 一個 10/100/1000 Base-T QRadar 管理介面 一個 10/100 Base-T 整合管理模組介面 兩個 10 Gbps SFP + 埠
記憶體	64 GB 8x 8 GB 1600 MHz RDIMM
儲存體	9 x 3.5 英吋 1 TB 7.2 K rpm NL SAS，總計 9 TB，6.2 TB 可用 (Raid 5)
電源供應器	雙重備用 750 瓦 AC 電源供應器
尺寸	深 29.5 英吋 x 寬 17.7 英吋 x 高 2.4 英吋

軟體需求

若要管理 Master Console，您必須使用 8500 啟動鍵 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 來安裝 IBM Security QRadar。您不需要個別的授權金鑰。

您可以使用 Master Console 監視 QRadar Log Manager 部署，但集中化攻擊管理視圖是空的。集中化攻擊管理視圖僅為監視攻擊的系統（如 QRadar SIEM）顯示攻擊。

管理 Master Console 所需的 QRadar 版本可能不同於 Master Console 可以監視的 QRadar 版本。在安裝 Master Console 之前，請檢閱下表中的軟體需求。

表 2. *Master Console* 的軟體需求

Master Console 版本	**安裝**	**監視**	**支援的瀏覽器**
Master Console 0.11.0 版*	隨 QRadar 7.2.8 版安裝。 無法在 IBM 修正程式中心 獨立下載 Master Console 0.11.0 版。	監視 QRadar 7.2.8 版或 7.2.7 版	Microsoft Internet Explorer 11 Mozilla Firefox 38 延伸支援版 Google Chrome（最新版本）
Master Console 0.10.0 版	在 QRadar 7.2.7 版上安裝。	監視 QRadar 7.2.6 版或 7.2.7 版	Microsoft Internet Explorer 11 Mozilla Firefox 38 延伸支援版 Google Chrome（最新版本）
Master Console 0.9.1 版	在 QRadar 7.2.6 版或 7.2.7 版 上安裝。	監視 QRadar 7.2.6 版或 7.2.7 版	Microsoft Internet Explorer 11 Mozilla Firefox 38 延伸支援版 Google Chrome（最新版本）
Master Console 0.9.0 版	在 QRadar 7.2.6 版上安裝。	監視 QRadar 7.2.6 版或 7.2.7 版	Microsoft Internet Explorer 11 Mozilla Firefox 38 延伸支援版 Google Chrome（最新版本）
Master Console 0.8.1 版	在 QRadar 7.2.5 版或 7.2.6 版 上安裝。	監視 QRadar 7.2.5 版或 7.2.6 版	Microsoft Internet Explorer 11 Microsoft Internet Explorer 10 Mozilla Firefox 38 延伸支援版 Google Chrome（最新版本）
* 產品支援限制用於 Master Console 的最新發行版本。			

如需安裝 QRadar 的相關資訊，請參閱《*IBM Security QRadar* 安裝手冊》。

安裝 Master Console 0.11.0 版

使用 8500 啟動鍵 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 安裝 IBM Security QRadar 7.2.8 版 之後，將自動安裝 Master Console。您無法獨立下載 Master Console 0.11.0 版。

如需安裝 QRadar 的相關資訊，請參閱《*IBM Security QRadar* 安裝手冊》。

安裝 Master Console 0.10.0 版或更舊版本

使用 8500 啟動鍵 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 安裝 IBM Security QRadar 7.2.5 版或更新版本之後，將自動安裝 Master Console。它不需要個別的授權金鑰。如需安裝 QRadar 的相關資訊，請參閱《*IBM Security QRadar* 安裝手冊》。

您可以從 IBM 修正程式中心 下載最新的 Master Console 特性及加強功能。

開始之前

請確保安裝所在的軟體驅動裝置符合需要的硬體規格。如需相關資訊，請參閱第 3 頁的『支援的環境』。

您必須具有檔案複製軟體程式（例如，WinSCP），以將 Master Console 修正套件檔案從您的本端系統複製到 QRadar 軟體驅動裝置。

關於這項作業

第一次更新至 Master Console 0.8.1 版或更新版本時，更新程序會從 QRadar Console 匯入使用者。匯入程序會改寫所有現有 Master Console 使用者（包括管理者）的密碼，並將它們設為 QRadar Console 上設定的相同密碼。匯入過程只會進行一次。Master Console 後續更新不會匯入使用者或改寫密碼。

程序

1. 從 Fix Central 中下載 Master Console 修正套件 (http://www.ibm.com/support/fixcentral.ibm.com/support/fixcentral)。
2. 使用軟體程式（例如，WinSCP），以將 Master Console 修正套件複製到您安裝 Master Console 的 QRadar 主機上。
3. 使用 SSH，以 root 使用者身分登入您在其中複製 Master Console 軟體修正程式的 QRadar 主機。
4. 透過鍵入下列指令，停止 Tomcat 服務：

   ```
   service tomcat stop
   ```

5. 在 QRadar 軟體驅動裝置的主控台視窗中，透過鍵入下列指令安裝 Master Console：

   ```
   yum -y install masterconsole-<version#>.rpm
   ```

6. 透過鍵入下列指令，重新啟動 Tomcat 服務：

   ```
   service tomcat start
   ```

結果

已安裝 Master Console，並已重新啟動 QRadar 軟體驅動裝置上的服務。

開啟 Master Console

安裝 Master Console 之後，可使用 QRadar Console 的 IP 位址來開啟 Master Console。

開始之前

請確保使用 8500 啟動鍵 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 安裝了 QRadar。

關於這項作業

第一次更新至 Master Console 0.8.1 版或更新版本時，更新程序會從 QRadar Console 匯入使用者。匯入程序會改寫所有現有 Master Console 使用者（包括管理者）的密碼，並將它們設為 QRadar Console 上設定的相同密碼。匯入過程只會進行一次。Master Console 後續更新不會匯入使用者或改寫密碼。

程序

1. 開啟 Web 瀏覽器，並鍵入下列 URL：

   `https://IP_address`

   其中 *IP_address* 是您安裝 Master Console 所在 QRadar 主機的 IP 位址。
2. 登入 Master Console。

   如果您是第一次登入 Master Console，請使用系統的管理者帳戶及 root 使用者密碼。

下一步

若要新增您要監視的 QRadar 部署，請參閱第 7 頁的『將部署新增至 Master Console』。

為 Master Console 建立授權記號

您必須建立授權記號以讓 Master Console 能夠連接至您的 IBM Security QRadar 部署。

程序

1. 在**系統配置**的**管理者**標籤上，按一下**授權的服務**。
2. 按一下**新增授權服務**，然後配置參數。
   a. 在**服務名稱**欄位中，鍵入服務的名稱。 此名稱的長度最多可為 255 個字元。
   b. 在**使用者角色**功能表中，選取**管理者**。

      指派給授權服務的使用者角色決定此服務在 QRadar 中可以存取的功能。Master Console 的授權記號必須具有**管理者**使用者角色。
   c. 在**安全設定檔**功能表中，選取**管理者**。

      安全設定檔會決定此服務在 QRadar 中可以存取的網路及日誌來源。Master Console 的授權記號必須具有**管理者**安全設定檔。
   d. 在**到期日期**欄位中，選取要使記號到期的日期，或按一下**無期限**勾選框。
3. 按一下**建立服務**，並記錄記號值。

將部署新增至 Master Console

Master Console 管理者必須新增您要監視的 IBM Security QRadar 部署。

開始之前

- 您必須具有授權記號。如需相關資訊，請參閱第 6 頁的『為 Master Console 建立授權記號』。
- 如果您的組織需要安全的 SSL，請確保在 Master Console 中將您要監視之所有 QRadar 部署中不受信任的 SSL 憑證取代為自簽憑證或授信憑證。
- 只有 QRadar 管理者才能在 Master Console 中新增、編輯或移除 QRadar 部署。

程序

1. 若要新增部署，請按一下畫面右上角的**新增**。
2. 鍵入部署的名稱。
3. 鍵入主控台 IP 位址或主機名稱。
4. 鍵入授權記號。
5. 按一下**新增部署**。
6. 如果您新增具有不安全 SSL 的部署，並且您的組織不需要安全的 SSL，請選取**忽略不安全的 SSL** 勾選框，然後按一下**新增部署**。

部署監視

Master Console 顯示與 Master Console 連接之每個 IBM Security QRadar 部署的性能及作業資料的圖形表示法，其稱為部署卡。

您可以在「依嚴重性列出部署」頁面上檢視部署卡。為幫助您快速判定需要注意的部署，部署卡分為三個群組：**嚴重**、**警告**及**良好**。

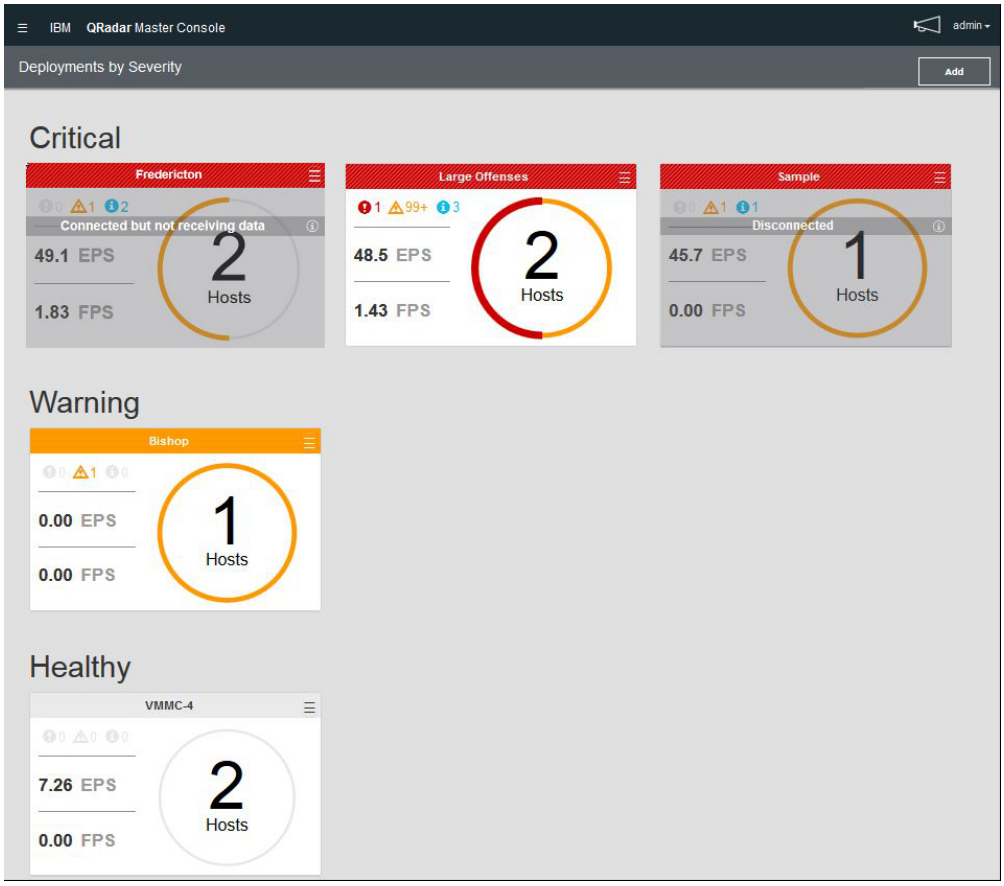

圖 *1. Master Console* 中的部署卡

每一個部署卡會顯示下列資訊：

- 部署中的受管理主機數目。
- 部署的狀態，以圍繞圓圈的顏色表示。例如，如果部署具有兩個受管理主機，且其中 1 個具有嚴重狀態，則圍繞數字 2 的圓圈一半是紅色。
- 最後 15 分鐘內的嚴重、警告及參考資訊系統通知數目。
- 事件與流程速率，以最後 15 分鐘的平均值進行測量。

當 Master Console 無法連接至部署時，部署卡會顯示**斷線**。此狀態可能表示部署已關閉電源。當部署顯示**已連接但未接收資料**時，可能授權記號已被撤銷或過期。

您可以對部署卡執行下列動作：

- 按一下部署卡可開啟**受管理主機**視圖。
- 按一下「漢堡」( ) 圖示可編輯部署詳細資料或中斷部署與 Master Console 的連線。
- 當部署為**斷線**或**已連接但未接收資料**時，按一下部署卡上的資訊圖示可查看前次接收資料的時間。

監視受管理主機

使用「受管理主機」頁面，可查看與單一部署連接之所有受管理主機的系統通知及系統記憶體與 CPU 使用率統計資料。

為幫助您快速判定需要注意的受管理主機，受管理主機卡的上面部分帶有顏色代碼：紅色指示**嚴重**狀態、黃色指示**警告**狀態，並且灰色指示**良好**狀態。

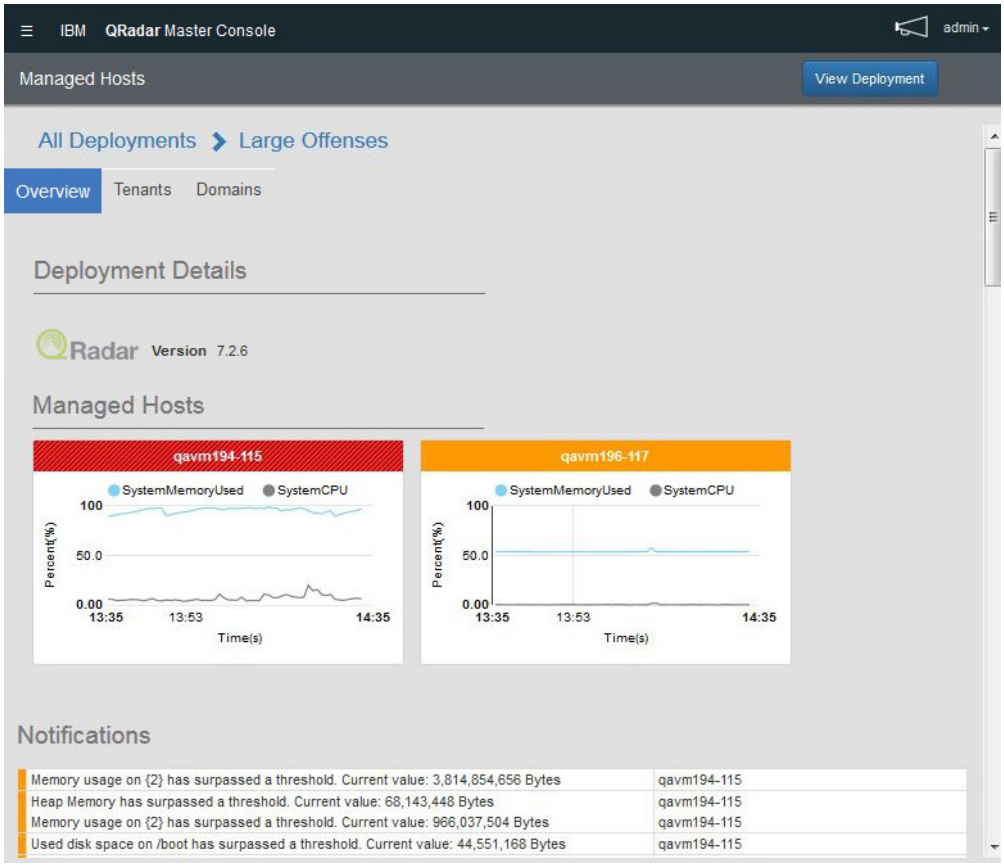

圖 2. *Master Console* 中的受管理主機頁面

程序

1. 若要檢視「受管理主機」頁面，請在「依嚴重性列出部署」頁面上按一下部署卡。
2. 在「受管理主機」頁面上，您可以執行下列動作：
   a. 按一下**檢視部署**可登入 QRadar 部署。
   b. 按一下**承租人**與**網域**標籤可檢視部署中所配置承租人與網域的相關資訊。
   c. 將滑鼠游標移至受管理主機圖形上方可檢視圖形度量值的相關資訊。
   d. 若要在受管理主機圖形上隱藏度量值，請按一下度量值的顏色圖示。例如，若要在圖形上隱藏 **SystemCPU** 度量值，請按一下**系統 CPU** 旁邊的灰色圓圈。
   e. 若要檢視主機的作業資料（如 CPU 與記憶體用量、網路與磁碟讀取及寫入以及事件與流程速率），請按一下受管理主機卡。

監視攻擊

使用 Master Console 來監視多個 IBM Security QRadar 部署的攻擊。所有部署的攻擊都顯示在單一清單中，並且最重要的攻擊顯示在最上面。

關於這項作業

攻擊卡依下列順序排序：長度、部署及前次更新的時間。

長度指示攻擊的相對重要性。其基於相關性、嚴重性及可靠性值進行計算。

- 相關性決定攻擊在您網路上的影響。例如，如果埠處於開啟狀態，則相關性很高。
- 可靠性指示攻擊的完整性，由日誌來源中配置的可靠性等級判定。當多個來源都報告同一事件，可靠性會增加。
- 嚴重性指示來源導致的威脅，與目的地應對攻擊的程度相關。

長度具有的數值可判定攻擊卡的顏色。將滑鼠游標移至攻擊卡的色軸上方，可查看長度數目。

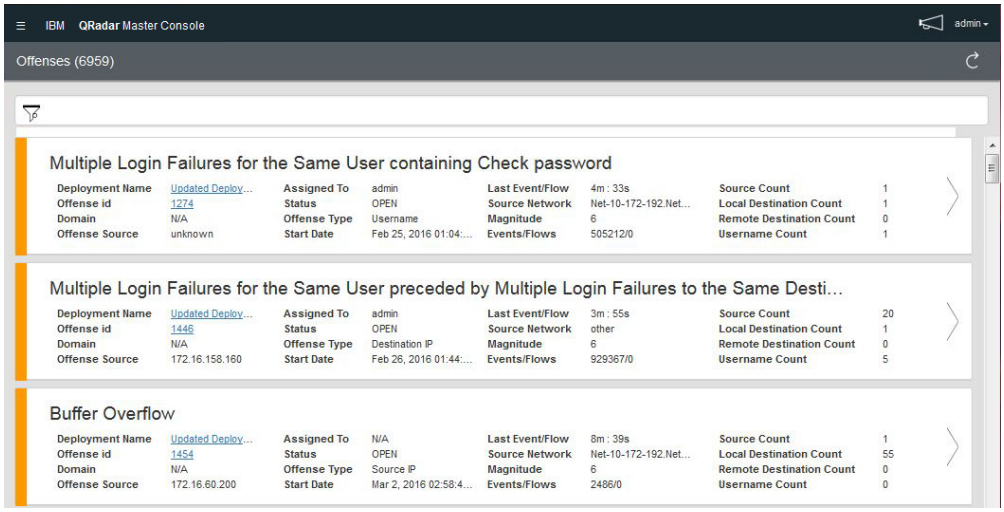

圖 3. *Master Console* 中的部署卡

部署卡顯示下列資訊：

表 3. 攻擊卡資訊

參數	說明
攻擊 ID	攻擊摘要的鏈結。
攻擊來源	攻擊來源資訊依賴於攻擊的類型。 例如，如果**攻擊類型**為「來源 IP」，則**攻擊來源**欄位會顯示建立攻擊之事件來源的 IP 位址。如果**攻擊類型**為「目的地 IP」，則**攻擊來源**欄位會顯示事件的目的地 IP 位址。
指派對象	如果未指派任何使用者來調查攻擊，您可以將攻擊指派給 QRadar 中的使用者。如需向 QRadar 指派攻擊的相關資訊，請參閱《*IBM Security QRadar* 使用手冊》。
狀態	依預設，過濾器僅顯示開啟的攻擊。

表 3. 攻擊卡資訊 (繼續)

參數	說明
攻擊類型	由建立攻擊的規則決定。 例如，如果攻擊類型為**日誌來源事件**，則產生攻擊的規則與基於偵測事件之裝置的事件產生關聯。
開始日期	指定與攻擊關聯之第一個事件或流程的指定日期和時間。
前次事件/流程	指定自前次觀察事件或流程的攻擊、種類、來源 IP 位址或目的地 IP 位址起經歷的時間。
來源網路	指定試圖中斷您網路上元件安全性的裝置的網路。
事件/流程	指定與來源 IP 位址、目的地 IP 位址、事件名稱、使用者名稱、MAC 位址、日誌來源、主機名稱、埠、日誌來源、ASN 位址、IPv6 位址、規則、ASN、應用程式、網路或種類相關聯的事件或流程的數目。
來源計數	指定與種類中的攻擊相關聯的來源 IP 位址的數目。如果來源 IP 位址與五種不同低層次種類的攻擊相關聯，則僅計算一次來源 IP 位址。

程序

1. 按一下左上角的「漢堡」圖示 ()，然後按一下**攻擊**。
2. 按一下攻擊卡上的箭頭鏈結，可登入部署並開啟攻擊摘要。
3. 若要檢視隱藏或關閉的攻擊，請按一下過濾  圖示，然後選取您要檢視之攻擊的勾選框。

   頁面標頭中會顯示符合已套用過濾器的攻擊數目。
4. 按一下重新整理圖示，以更新所列的攻擊。

相關工作:

第 6 頁的『開啟 Master Console』
安裝 Master Console 之後，可使用 QRadar Console 的 IP 位址來開啟 Master Console。

過濾攻擊清單

建立搜尋查詢來過濾合併攻擊清單中顯示的攻擊卡。例如，您可以過濾攻擊清單以僅顯示那些指派給一個個體的攻擊，或者您可以過濾以僅顯示單一部署的攻擊。

關於這項作業

您使用**攻擊**視圖上的全文搜尋欄位可快速尋找已關閉或完全相符的攻擊，並以排好的順序顯示。您可以建立查詢來尋找一個單字、單字的一部分或以精確順序或任何順序排列的多個單字。您可以搜尋攻擊卡上所有資料欄位中的資料，也可以指定您要搜尋的 ID 來縮小搜尋。

全文搜尋功能基於 Apache Lucene 搜尋引擎。搜尋不區分大小寫。若要對單一字元使用萬用字元進行搜尋，請使用 ? 符號。若要對多個字元使用萬用字元進行搜尋，請使用 * 符號。

您可以指定攻擊卡上要搜尋的欄位來縮小搜尋。下表顯示攻擊卡上的欄位的欄位 ID：

表 *4.* 攻擊卡上用於搜尋資料的欄位 *ID*

攻擊卡說明	**欄位 ID**
攻擊說明	說明
部署名稱	deployment_name
攻擊 ID	offense_id
網域	domain_id
攻擊來源	offense_source
指派給	assigned_to
狀態	status
攻擊類型	offense_type 您無法使用萬用字元來搜尋 `offense_type`。您必須在查詢中指定完全相符的文字。
開始日期	start_time
前次事件/流程	last_updated_time
來源網路	source_network
長度	magnitude
事件/流程	event_count flow_count
來源計數	source_count
本端目的地計數	local_destination_count
遠端目的地計數	remote_destination_count
使用者名稱計數	username_count

程序

1. 按一下左上角的「漢堡」圖示 ()，然後按一下**攻擊**。
2. 在搜尋欄位中，鍵入您要搜尋之文字的搜尋查詢。
   - 若要搜尋攻擊卡上顯示的任何資料，請在搜尋方框中鍵入文字。
   - 若要搜尋特定欄位中的資料，請鍵入欄位 ID，後跟冒號，然後是您要搜尋的詞彙。
   - 若要跳出特殊字元，請在搜尋查詢的下列字元之前使用 \：
     `+ - && || ! ( ) { } [ ] ^ " ~ * ? : \`

   搜尋查詢範例：

   下表顯示您可以用於在攻擊卡搜尋資料的查詢範例：

表 *5. Master Console* 搜尋表示式

說明	**搜尋查詢**
搜尋任意欄位中包含 `text` 或 `test` 的攻擊。	`te?t`
搜尋包含 `test`、`tests` 或 `tester` 的攻擊。	`test*`

表 5. *Master Console* 搜尋表示式 (繼續)

說明	搜尋查詢
搜尋任意欄位中包含 password 的攻擊。	*password*
搜尋長度等級為 2、3 或 4 的攻擊。	magnitude:[2 to 4]
搜尋長度等級為 3 或 5 的攻擊。	magnitude:(3 OR 5)
搜尋「攻擊類型」等於 Event Name 的攻擊。	offense_type: "Event Name"
搜尋自現在起過去 10 天內更新的攻擊。	last_update_time:[NOW-10DAYS to NOW]
搜尋 Bishop 部署中長度為 3 的攻擊。	deployment_name:Bishop AND magnitude:3

3. 若要檢視隱藏或關閉的攻擊，請按一下過濾圖示 ()，然後選取您要查看之攻擊的勾選框。

   頁面標頭中會顯示符合已套用過濾器的攻擊數目。

使用者管理

在 Master Console 中可直接管理 Master Console 使用者。

第一次更新至 Master Console 0.8.1 版或更新版本時，更新程序會從 QRadar Console 匯入使用者。匯入過程只會進行一次。Master Console 後續更新不會匯入使用者。在起始匯入之後，可從 Master Console 直接管理所有使用者帳戶。

新增本端使用者

安裝 Master Console 並更新至最新版本之後，管理者可以直接在 Master Console 中新增使用者。

程序

1. 按一下左上角的「漢堡」圖示 ()，然後按一下**設定**。
2. 按一下**使用者管理**。
3. 在「使用者管理」視窗的右上角，按一下**新增**以開啟「新增使用者」視窗。
4. 輸入新使用者的資訊。
5. 如果新使用者是管理者，請按一下**安全管理者**勾選框。
6. 按一下**新增使用者**。

編輯使用者設定

在 Master Console 中變更本端使用者的設定，例如使用者密碼。

關於這項作業

IBM Security QRadar 中變更的本端使用者密碼不會自動套用至 Master Console。您必須在 Master Console 中編輯使用者設定並變更密碼。

您不能在 Master Console 中變更 LDAP 及 Active Directory 密碼。

程序

1. 按一下左上角的「漢堡」圖示 ()，然後按一下**設定**。
2. 按一下**使用者管理**。
3. 在您要編輯之使用者的卡上，按一下「漢堡」功能表  圖示。
4. 選取**編輯使用者**。
5. 在編輯使用者視窗上，修改使用者資訊。
6. 按一下**編輯使用者**以儲存您的變更。

移除本端使用者

如果使用者不再需要存取，請從 Master Console 移除該本端使用者。

程序

1. 按一下左上角的「漢堡」圖示 ()，然後按一下**設定**。
2. 按一下**使用者管理**，以檢視所有本端使用者的卡。
3. 在您要編輯之使用者的卡上，按一下「漢堡」功能表  圖示。
4. 選取**移除使用者**。
5. 在確認視窗中，選取**移除使用者**。

過濾使用者清單

建立搜尋查詢來過濾「使用者管理」頁面上顯示的 Master Console 使用者清單。例如，您可以過濾使用者清單以僅顯示作用中的使用者，或者您可以過濾以僅顯示具有管理安全設定檔的使用者。

關於這項作業

您使用「使用者管理」視圖上的全文搜尋欄位可快速尋找已關閉或完全符合搜尋準則的使用者。全文搜尋功能基於 Apache Lucene 搜尋引擎。若要對單一字元使用萬用字元進行搜尋，請使用問號 (?)。若要對多個字元使用萬用字元進行搜尋，請使用星號 (*)。您可以指定要搜尋的使用者欄位來縮小搜尋。

程序

1. 按一下左上角的「漢堡」圖示 ()，然後按一下**設定**。
2. 按一下**使用者管理**。
3. 在搜尋欄位中，鍵入您要搜尋之文字的搜尋查詢。
   - 若要搜尋開放式文字，請在搜尋方框中鍵入文字。您必須在開放式搜尋中使用完整單字。您不能使用部分單字或萬用字元。
   - 若要搜尋特定欄位中的資料，請鍵入欄位 ID，後跟冒號，然後鍵入您要搜尋的詞彙。

搜尋查詢範例：

下表顯示您可以用於搜尋使用者資料的查詢範例：

表 *6.* 使用者資料搜尋表示式

說明	搜尋字串
搜尋**使用者名稱**欄位中的文字。	`name:John`
搜尋唯一登入名稱。搜尋此欄位時區分大小寫。	`login:Coop1`
搜尋電子郵件位址。 您必須提供完整的電子郵件位址。您無法搜尋部分電子郵件位址。	`email:coop1@ca.ibm.com`
搜尋系統上目前處於作用中的使用者。	`status:ACTIVE`
搜尋具有管理專用權的所有使用者。	`role_name:admin`
搜尋前 14 天對設定檔進行了修改的使用者。	`last_modified:[NOW-14DAYS TO NOW]`

在 Master Console 中配置 Active Directory 及 LDAP 鑑別

第一次配置 Microsoft Active Directory 或 LDAP 鑑別提供者時，您必須將範圍資訊新增至 `/opt/qradar/masterconsole/conf/shiro.realms` 檔案。

如果您最近已升級至 Master Console 0.10.0 版，您必須將範圍資訊從 `shiro.ini` 備份檔手動複製到 `/opt/qradar/masterconsole/conf/shiro.realms` 檔案。Master Console 在未來升級時會保留這些範圍資訊。

開始之前

確認 `/opt/qradar/masterconsole/conf/` 目錄中存在 `shiro.ini.<timestamp>` 備份檔。如果備份檔不存在，請建立一個。

檢閱鑑別伺服器上的配置。視配置的鑑別提供者的類型而定，您可能需要提供下列參數值：

表 *7.* 鑑別參數說明

參數	說明
`searchBase`	組織使用者所在之 Active Directory 或 LDAP 目錄的根目錄。
`searchFilter`	用來尋找 Active Directory 或 LDAP 使用者的環境定義。帳戶是由大多數伺服器使用的預設物件類別，但此項目可根據特定 Active Directory 或 LDAP 伺服器配置而改變。
`groupAttribute`	識別 Active Directory 或 LDAP 使用者屬於的使用者群組。
`groupRolesMap`	Active Directory 或 LDAP 群組與 Apache Shiro 角色的對映。
`userDnTemplate`	從 Active Directory 或 LDAP 伺服器擷取使用者的 DN 範本。
`contextFactory.url`	Active Directory 或 LDAP 伺服器 IP 位址及埠號。

表 7. 鑑別參數說明 (繼續)

參數	說明
principalSuffix	指定主要字尾以簡化使用者必須指定的登入資訊。 例如，您可以建立稱為 canada 的使用者主要字尾，然後使用者可鍵入 username@canada，而不是 username@this.is.my.long.domain.name.in.canada.com。

程序

1. 切換至 /opt/qradar/masterconsole/conf/ 目錄。
2. 製作 shiro.realms 檔案的副本：

   ```
   cp shiro.realms.default shiro.realms
   ```

3. 開啟 shiro.realms 檔案。
4. 若要配置 Microsoft Active Directory，請執行下列步驟：
   a. 找到下列區段，並將範例值取代為您鑑別環境的值：

   ```
   # ----------------------------------------------------------------------------
   # 下列區段用於配置 ActiveDirectory 範圍。在範例值
   # 新增至 securityManager.realm 之前予以取代
   # ----------------------------------------------------------------------------
   adRealm = org.apache.shiro.realm.activedirectory.ActiveDirectoryRealm
   adRealm.url = ldap://{ad_server}:389
   adRealm.groupRolesMap = "CN=the_users,CN=Users,DC=department,DC=company,DC=com":"admin"
   adRealm.searchBase = "DC=department,DC=company,DC=com"
   adRealm.systemUsername= user_name
   adRealm.systemPassword= password
   adRealm.principalSuffix= @company.com
   ```

   b. 將 $adRealm 新增至 securityManager.realms 項目：

   ```
   securityManager.realms = $localRealm, $adRealm
   ```

5. 若要配置 LDAP，請執行下列步驟：
   a. 找到下列區段，並將範例值取代為您鑑別環境的值：

   ```
   #----------------------------------------------------------------------------
   # 下列區段用於配置 OpenLdap 範圍。在範例值
   # 新增至 securityManager.realm 之前予以取代
   #----------------------------------------------------------------------------
   ldapRealm = com.ibm.si.mc.security.shiro.realm.LdapRealm
   ldapRealm.searchBase = "dc=company,dc=com"
   ldapRealm.searchFilter = (&(objectClass=account)(uid={0}))
   ldapRealm.groupAttribute = ou
   ldapRealm.groupRolesMap = "Manager":"admin"
   ldapRealm.userDnTemplate = uid={0},dc=company,dc=com
   ldapRealm.contextFactory.url = ldap://{ldap_server}:389
   ```

   b. 將 $ldapRealm 新增至 securityManager.realms 項目：

   ```
   securityManager.realms = $localRealm, $ldapRealm
   ```

6. 儲存 /opt/qradar/masterconsole/conf/shiro.realms 檔案。
7. 鍵入下列指令，以將範圍資訊新增至 shiro.ini 檔案：

   ```
   /opt/qradar/masterconsole/bin/generateShiroIni.py
   ```

8. 透過使用下列指令，重新啟動 tomcat 伺服器：

   ```
   service tomcat restart
   ```

下一步

使用 Microsoft Active Directory 或 LDAP 鑑別登入 Master Console，以測試配置。

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，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。 本文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、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 Corporation
North 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

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。

4544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。這些網站上的內容並非本 IBM 產品內容的一部分，貴客戶使用這些網站時應自行承擔風險。

IBM 得以各種 IBM 認為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為了 (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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785US

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。

執行效能資料和引用的客戶範例僅供說明之用。實際效能結果可能依特定的配置和作業條件而改變。

本文件所提及之非 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 未來方向或意圖的陳述僅代表其目標，如有變更或撤銷並不會另行通知。

所有 IBM 價格為 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。 為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，如與實際人名或企業有任何類似之處，純屬巧合。

商標

IBM、IBM 標誌及 ibm.com® 是 International Business Machines Corp. 在世界許多管轄區註冊的商標或註冊商標。其他產品及服務名稱可能是 IBM 或其他公司的商標。IBM 商標的最新清單可在 Web 的 "Copyright and trademark information" 中找到，網址為 www.ibm.com/legal/copytrade.shtml。

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。

產品說明文件的條款

這些出版品的使用許可權係遵循下列條款而授予。

適用範圍

下列條款係 IBM 網站使用條款之特別條款。

個人使用

貴客戶可以為了非商務性的私人用途而複製這些出版品，但必須保留所有專利注意事項。未經 IBM 明示同意， 貴客戶不得散佈、顯示或製作這些出版品或其任何部分的衍生著作。

商業使用

貴客戶可以在企業內複製、散布和顯示這些出版品，但必須保留所有專利注意事項。未經 IBM 明示同意，貴客戶不得製作這些出版品的衍生著作，也不得於企業外重製、散佈或顯示這些出版品或其任何部分。

權利

除了本項許可權所明確授予者之外，並未明示或暗示授予出版品或任何資訊、資料、軟體或其中的其他智慧財產的任何其他許可權、授權或權利。

若 IBM 審慎評估後認為本出版品用途已危及其利益，或 IBM 認為上述指示未被適當遵循，IBM 保留隨時撤銷此許可聲明的權利。

除非完全符合所有適當的法律和規章，其中包括所有美國輸出法律和規章，否則，貴客戶不能下載、輸出或再輸出本項資訊。

IBM 不提供這些出版品內容的任何保證。這些出版品只依「現狀」提供，不含任何明示或暗示的保證，其中包括且不限於可售性或符合特定效用的暗示保證。

IBM 線上隱私權聲明

IBM 軟體產品（包括作為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為了其他目的。 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啟用的功能。

如果為此「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（網址為 http://www.ibm.com/privacy ），以及 IBM 的線上隱私權條款（網址為 http://www.ibm.com/privacy/details），以及「IBM 軟體產品及軟體作為服務隱私權條款」（網址為 http://www.ibm.com/software/info/product-privacy）。

隱私權條款考量

IBM 軟體產品（包括作為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為了其他目的。 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啟用的功能。

如果為此「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（網址為 http://www.ibm.com/privacy ），以及 IBM 的線上隱私權條款（網址為 http://www.ibm.com/privacy/details），以及「IBM 軟體產品及軟體作為服務隱私權條款」（網址為 http://www.ibm.com/software/info/product-privacy）。

Printed in Taiwan