IBM Security QRadar Incident Forensics
版本 7.3.0

QRadar Packet Capture 使用手册

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。

產品資訊

本文件適用於 IBM QRadar Security Intelligence Platform 7.3.0 版 及後續發行版，直至有本文件的更新版本替代為止。

目錄

關於本 Packet Capture 使用手冊

本文件為您提供安裝與配置 IBM® QRadar® Packet Capture 所需的資訊。

讀者對象

負責安裝 QRadar Packet Capture 的系統管理者必須熟悉網路安全概念及裝置配置。

技術說明文件

若要在 QRadar 產品檔案庫中尋找 IBM Security QRadar 產品說明文件，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?uid=swg21616144)。

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。

第 1 章 QRadar Packet Capture 簡介

IBM Security QRadar Packet Capture 是網路資料流量擷取及搜尋應用程式。 QRadar Packet Capture 軟體驅動裝置只有一個擷取埠 (DNA0)，您只能安裝 10G 或 1G SFP 收發器。

使用 QRadar Packet Capture，您可以透過線上網路接口以每秒高達 10 Gbps 的速率來擷取網路封包，並將其寫入檔案而不流失封包。

您可以使用 QRadar Packet Capture 依時間與封包封套資料來搜尋擷取的網路資料流量。憑藉充分的軟體驅動裝置資源及自訂搜尋，您可以同步使用搜尋及錄製器資料而不會流失資料。

較之單個的獨立式伺服器，擁有 10G 收發器的 QRadar Packet Capture 軟體驅動裝置支援叢集擴大整體資料儲存體容量及計算能力。擁有 1G 收發器的 QRadar Packet Capture 軟體驅動裝置不支援叢集。

QRadar Packet Capture 功能

QRadar Packet Capture 包含的部分功能：

標準 PCAP 檔案格式

用於儲存網路資料流量的檔案格式。 該檔案格式與現有的第三方分析工具相整合。

高效能的封包至磁碟記錄

從現用網路中擷取網路封包。

多核心支援

QRadar Packet Capture 設計用於多核心架構。

直接 IO 磁碟存取

QRadar Packet Capture 使用直接 IO 存取磁碟來達到磁碟寫傳輸量的上限。

即時索引

QRadar Packet Capture 可以在封包擷取期間自動產生索引。 您可以使用「Berkeley 封包過濾器 (BPF)」的語法及／或 HTTP 網域或基本 URL 來查詢索引，以快速擷取您所感興趣的指定時間間隔內的封包。

能夠增加擷取資料容量的叢集（僅限 10G 版本）。

您可以啟用資料節點來為新增的儲存體容量建立叢集。

傾出格式

Capture 檔案以標準的 PCAP 格式儲存，並使用微秒時間戳記解決方案。 Capture 檔案依檔案大小順序儲存。 Capture 檔案儲存在目錄中。 若目錄中的空間變滿，則會根據預先配置的記錄參數改寫 Capture 檔案。

擷取速度

對於封包擷取軟體驅動裝置，擷取網路資料流量的速度取決於您是否有資料節點連接至主要節點：

- 對於未連接資料節點的封包擷取軟體驅動裝置，擷取速度上限可達 7 Gbps。
- 對於包含已連接主要節點之資料節點的封包擷取軟體驅動裝置，擷取速度上限可達 10 Gbps。

如需將封包轉遞至 QRadar Packet Capture 的相關資訊，請參閱《*IBM Security QRadar* 管理手冊》。

相關概念:

第 9 頁的第 3 章, 『Capture 使用概觀』

若要擷取磁碟的資料流量，請啟動擷取應用程式。 「記錄器」元件會將網路資料流量資料儲存至預先配置的目錄中。 若目錄中的空間變滿，則會改寫現有檔案。

第 2 章 QRadar Packet Capture 設定

在使用 IBM Security QRadar Packet Capture 之前，需要執行部分基本配置。

支援的 Web 瀏覽器

支援下列 Web 瀏覽器：

- Google Chrome 44.0.2403.157 版或更新版本。
- Mozilla Firefox 40.0.3 版或更新版本。

設定網路

若要遠端使用 QRadar Packet Capture，則必須將 IP 位址指定為其中一個乙太網路埠，一般是 eth2、eth3 或 eth4。 依預設，系統配置為使用 DHCP。 如需起始配置，您可能需要連接 VGA 相容的監視器。

對於起始配置，請執行下列步驟：

1. 開啟 QRadar Packet Capture 軟體驅動裝置。
2. 以 root 使用者身分使用 SSH 和埠 4477 登入。

   預設使用者名稱為 root。預設密碼為 P@ck3t08..。

   若要變更預設密碼，請參閱第 5 頁的『變更作業系統帳戶密碼』。
3. 為了確保您的系統保持最新，請套用 IBM Fix Central (www.ibm.com/support/fixcentral/) 上提供的軟體修正程式。
4. 配置您的專屬網路的靜態 IP 位址：
   a. 若要取得 MAC 位址或 eth2 介面，請輸入下列指令：

      ```
      ifconfig | grep eth2
      ```

      介面 eth0 和 eth1 無法使用。 對於 M4 xSeries 硬體，請使用 eth2。
   b. 請記錄 MAC 位址。
   c. 編輯 /etc/sysconfig/network-scripts/ifcfg-eth2 檔中的設定：
      - 將下列文字新增為第一行：DEVICE=eth2
      - 解除註解 eth2 埠的 MAC 位址：HWADDR=xx:xx:xx:xx:xx
      - 確保配置下列設定：BOOTPROTO=static
      - 確保使用您網路的相關資訊，輸出類似下列靜態範例：

        ```
        DEVICE=eth2
        #HWADDR=xx:xx:xx:xx:xx
        BOOTPROTO="static"
        BROADCAST="192.168.1.255"
        DNS1="0.0.0.0"
        DNS2="0.0.0.0"
        GATEWAY="192.168.1.2"
        IPADDR="192.168.1.1"
        NETMASK="255.255.255.0"
        NM_CONTROLLED="no"
        ONBOOT="yes"
        ```

5. 儲存檔案。
6. 若要套用設定，請執行下列指令：

   ```
   service network restart
   ```

7. 請執行下列指令來驗證您的介面設定：

   ```
   ifconfig | more
   ```

DHCP 範例：在 CentOS6.2 中，編輯 /etc/sysconfig/network-scripts/ifcfg-eth0 檔案或 /etc/sysconfig/network-scripts/ifcfg-eth1 檔案中的下列設定。

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

遠端登入

本端設定 IP 位址之後，您可以使用 SSH 在埠 4477 上遠端登入，以管理軟體驅動裝置。

配置授權

在您使用 QRadar Packet Capture 之前，必須配置 QRadar Packet Capture 軟體驅動裝置和 QRadar Packet Capture 軟體的授權。

程序

1. 若要配置已安裝 SFP 1G 收發器的 QRadar Packet Capture 軟體驅動裝置的授權，請完成下列步驟：
   a. 請聯絡您的 IBM 代表，以取得主節點的授權金鑰。
   b. 在 QRadar Packet Capture 中，按一下**說明** > **更新主要授權**。
   c. 若要向 QRadar Packet Capture 軟體驅動裝置套用授權，請將值貼至**授權金鑰**欄位。
   d. 將**系統 ID** 和**授權金鑰**的值貼至各自的欄位。
   e. 按一下**更新主要授權**以套用變更。
2. 若要配置已安裝 SFP+ 10G 收發器的 QRadar Packet Capture 軟體驅動裝置的授權，請完成下列步驟：
   a. 請聯絡您的 IBM 代表，以取得資料節點的授權金鑰。
   b. 在 QRadar Packet Capture 中，若要套用主要授權，請按一下**說明** > **更新主要授權**。
   c. 將**授權**和**系統 ID** 的值貼至各自的欄位。
   d. 按一下**更新主要授權**以套用變更。
   e. 根據您在叢集中擁有的資料節點數，您需要按一下**說明** > **Node1**。
   f. 若要更新資料節點授權，請將**授權金鑰**和**系統 ID** 的值貼至各自的欄位。
   g. 若要更新資料節點，請按一下**更新 Node1 授權**以套用變更。

管理使用者

若要使使用者能夠存取和使用 IBM Security QRadar Packet Capture，必須新增使用者、為使用者指派適當的角色並配置使用者的登入認證。

開始之前

確保已以 root 使用者的身分登入 QRadar Packet Capture。或者請確保您可以使用 sudo 指令來建立使用者。

程序

1. 若要建立使用者，請執行下列指令：

   ```
   ./usr/local/nc/bin/nc_user_manager add <username> <password> <Admin|Guest>
   ```

   如果已有名為 *<username>* 的使用者，此指令將會失敗。

   如果所指定的角色既不是管理者又不是訪客，此指令將會失敗。

   新增使用者後，您可以將相同的使用者名稱和密碼用於產品登入和 REST API 登入。
2. 若要刪除使用者，請執行下列指令：

   ```
   ./usr/local/nc/bin/nc_user_manager delete <username> <password>
   ```

   如果已有名為 *<username>* 的使用者，此指令將會失敗。

   如果 *<username>* 和 *<password>* 與 QRadar Packet Capture 中記錄的使用者名稱和密碼不符，此指令將會失敗。

   刪除使用者後，您可以將相同的使用者名稱和密碼用於產品登入和 REST API 登入。

變更作業系統帳戶密碼

設定軟體驅動裝置之後，請變更 IBM Security QRadar Packet Capture 的預設作業系統密碼。

您必須是 root 使用者才能變更作業系統帳戶。

QRadar Packet Capture 應用程式密碼是獨立於作業系統密碼的。

程序

1. 以 root 使用者身分使用 SSH 登入。

   root 使用者的預設密碼是 P@ck3t08..
2. 若要變更 root 使用者帳戶的密碼，請使用 **passwd** *username* 指令。

同步化 QRadar Packet Capture 伺服器時間與 QRadar 主控台 系統時間

若要確保 IBM Security QRadar 具有一致的時間設定，以便搜尋及與資料相關的功能可以正常工作，每個軟體驅動裝置都必須與 QRadar 主控台 軟體驅動裝置同步化。管理者必須更新 QRadar 主控台 軟體驅動裝置上的 iptables，然後將它配置成接受埠 37 上的 rdate 通訊。

開始之前

您必須知道 QRadar 主控台 的 IP 位址或主機名稱。 主機名稱必須使用 nslookup 正確解析。

依預設，QRadar Packet Capture 裝置的時區設定為 UTC（國際標準時間）。

程序

1. 使用 SSH，以 root 使用者的身分登入 QRadar Packet Capture 軟體驅動裝置。
2. 若要關閉網路時間通訊協定 (NTP) 服務，請輸入下列指令：`service ntpd stop`。
3. 若要關閉 NTP 的檢查配置，請輸入下列指令：`chkconfig ntpd off`。
4. 透過編輯 crontab (crontable) 檔案將同步化排程為 cron 工作。
   a. 輸入下列指令：`crontab -e`。
   b. 若要將軟體驅動裝置配置成每 10 分鐘與 QRadar 主控台同步化一次，請輸入下列指令：`*/10 * * * * rdate -s` *`Console_IP_Address`*。

      對於 *Console_IP_Address* 變數，可以使用 IP 位址或主機名稱。
   c. 儲存配置變更。
   d. 透過輸入下列指令，開啟 crond：

      ```
      service crond start
      chkconfig crond on
      ```
5. 更新 QRadar 主控台 上的 iptables 以接受來自 QRadar Packet Capture 裝置的 rdate 資料流量。
   a. 使用 SSH，以 root 使用者的身分登入 QRadar 主控台 軟體驅動裝置。
   b. 編輯 /opt/qradar/conf/iptables.pre 檔案。
   c. 輸入下列指令：

      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
      ```

      如果您有多個 QRadar Packet Capture 軟體驅動裝置，請一行新增一個 IP 位址。

      範例：

      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```
   d. 儲存 iptables.pre 檔案。
   e. 透過輸入下列指令，更新 QRadar 主控台 上的 iptables：

      ```
      ./opt/qradar/bin/iptables_update.pl
      ```

相關概念:

第 9 頁的第 3 章, 『Capture 使用概觀』
若要擷取磁碟的資料流量，請啟動擷取應用程式。 「記錄器」元件會將網路資料流量資料儲存至預先配置的目錄中。 若目錄中的空間變滿，則會改寫現有檔案。

第 3 章 Capture 使用概觀

若要擷取磁碟的資料流量，請啟動擷取應用程式。 「記錄器」元件會將網路資料流量資料儲存至預先配置的目錄中。 若目錄中的空間變滿，則會改寫現有檔案。

疑難排解： 如果您看到未收集任何資料，請確保連線上有資料流量。 若要擷取資料流量，必須使用 Tap 或 SPAN（鏡映）埠。 使用交換器上的 SPAN 埠時，如果交換器將較低的優先順序指派給 SPAN 埠，可能會捨棄一些封包。

入門

設定系統之後，請執行下列步驟來登入 IBM Security QRadar Packet Capture：

1. 開啟 Web 瀏覽器並鍵入下列 URL：

   `https://PCAP_IP_Address:41390`

2. 使用下列使用者帳戶資訊登入：

   使用者：`continuum`

   密碼：`P@ck3t08..`

疑難排解：如果使用者在 10 分鐘之內無法連續五次給出正確的密碼，則使用者將鎖出 30 分鐘。系統管理者可以手動解除鎖定使用者帳戶。

依預設，會顯示「Capture 狀態」頁面。 您可以按一下**啟動 Capture**或**停止 Capture**，來控制記錄。

Capture 狀態

「Capture 狀態」頁面上提供下列資訊：

- **介面擷取位置**
- **Capture 狀態**
- **啟動/停止時間**
- **擷取系統的持續時間**
- **傳輸率**
- **擷取的封包**
- **已擷取位元組數**
- **捨棄的封包**
- **可用的儲存空間**

在叢集配置中，針對每一個已啟用的資料節點，顯示儲存體使用率。 如果因為網路配置問題或連線不當導致無法存取 QRadar Packet Capture Data Node，而不是因為儲存體統計資料所致，則會顯示下列訊息：`Slave node is enabled but is currently unreachable`（已啟用從屬節點，但目前無法存取）。

疑難排解

若要檢查已配置擷取介面的相關系統資訊，請按一下**疑難排解**。

伺服器資訊

若要檢查伺服器儲存體資訊，請按一下**伺服器資訊**。

網路特性

以圖形格式檢視網路的傳輸量。

擷取到磁碟的預設傳輸量上限是 10 Gbps。

擷取歷程

檢視已發生或正在發生的封包擷取歷程。

行內壓縮

為了支援取證調查，您可以透過增大可用虛擬儲存空間容量而不新增實體磁碟，來將原始封包內容保留較長的持續時間。 現在，您可以使用新的行內壓縮選項來將較大量的資料儲存在 QRadar Packet Capture 軟體驅動裝置上。

壓縮量與有效負載中的已壓縮視訊內容量相關。例如，如果您的有效負載中有 5% 的壓縮視訊，則壓縮比例是 13:1。 壓縮：儲存空間比例是未經壓縮的大小與壓縮後的大小之間的比例。

表 *1.* 行內壓縮率

已壓縮視訊有效負載的百分比 (%)	壓縮:儲存空間放大率
0	17:1
5	13:1
10	6:1
20	4:1
40	2.4:1

相關概念:

第 1 頁的第 1 章, 『QRadar Packet Capture 簡介』
IBM Security QRadar Packet Capture 是網路資料流量擷取及搜尋應用程式。 QRadar Packet Capture 軟體驅動裝置只有一個擷取埠 (DNA0)，您只能安裝 10G 或 1G SFP 收發器。

相關工作:

第 6 頁的『同步化 QRadar Packet Capture 伺服器時間與 QRadar 主控台 系統時間』
若要確保 IBM Security QRadar 具有一致的時間設定，以便搜尋及與資料相關的功能可以正常工作，每個軟體驅動裝置都必須與 QRadar 主控台 軟體驅動裝置同步化。管理者必須更新 QRadar 主控台 軟體驅動裝置上的 iptables，然後將它配置成接受埠 37 上的 rdate 通訊。

第 4 章 叢集

使用 QRadar Packet Capture 軟體驅動裝置來作為獨立式單個伺服器，或伺服器叢集。

較之單個獨立式伺服器，10G 修訂版本支援叢集擴大整體資料儲存體容量及計算能力。叢集包含一個主要裝置。您可以最多將兩個 QRadar Packet Capture 資料節點連接至每一個 QRadar Packet Capture 主要系統。

叢集標籤顯示兩個資料節點，及其現行狀態。

依預設，資料節點不屬於叢集，且狀態為已停用。

啟用資料節點

將 IBM Security QRadar Packet Capture 資料節點實際連接至 QRadar Packet Capture 主要節點之後，必須啟用 QRadar Packet Capture 資料節點。 啟用和連接 QRadar Packet Capture 資料節點將會建立一個叢集，以用於新增的儲存體容量和加強的擷取效能。

如需連接軟體驅動裝置的相關資訊，請參閱《*QRadar Packet Capture* 快速參照手冊》。

開始之前

確保擷取程式伺服器正在執行。

程序

1. 若要啟用資料節點，請遵循下列步驟：
   a. 在**叢集**標籤中，對每一個資料節點，選取**啟用**。狀態顯示**已連接**。
   b. 重新啟動擷取程式伺服器。現在，已啟用 QRadar Packet Capture Data Node。

   如果 QRadar Packet Capture 資料節點已連接且在執行中，則叢集中它們的狀態變更為「已連接」。

   主要節點連接至資料節點之後，儀表板上顯示的壓縮（虛擬）儲存體大小包括已連接資料節點的儲存體大小。
2. 若要停用資料節點，請遵循下列步驟：
   a. 在「叢集」標籤中，對每一個資料節點，選取**停用**。狀態顯示**已斷線**。
   b. 重新啟動擷取程式伺服器。QRadar Packet Capture 資料節點現在已停用，且無法再與主要系統相關聯。

   斷線的資料節點不再儲存資料。

   停用主要節點之後，儀表板上的壓縮（虛擬）儲存體大小會降低。

   如果已授權 Data Node1 或 Data Node2，則授權直欄顯示**永久**或**評估**，取決於您使用的授權。

第 5 章 QRadar Packet Capture 圖

在 IBM Security QRadar Packet Capture 中，使用實時或歷程圖來視覺化封包擷取統計資料。

實時圖

實時圖會追蹤現行封包擷取的下列相關封包擷取統計資料：

- 傳輸量（單位：Gbps，每秒千兆位數）
- 每秒封包總數
- 每秒 TCP 封包數
- 每秒 UDP 封包數
- 每秒非 UDP 封包資料流量
- 系統事件數
- 封包壓縮比例

將滑鼠移至圖形，並取得圖形上該點的統計資料。

您可以按一下圖形復原點，並自動產生搜尋要求。您也可以按一下顯示樣式圖示，以變更圖形的檢視。

歷程圖形

歷程圖形可提供封包擷取歷程的長期概觀。歷程時間表選項包括 1 小時、1 天和 1 週。

將滑鼠移至圖形，並取得圖形上該點的統計資料。

您可以按一下圖形復原點，以自動產生搜尋要求。

第 6 章 搜尋某段時間範圍內的封包，以進行診斷測試

擷取時所建立的索引資料用於產生封包擷取 (pcap) 檔案，該檔案包含符合指定時間範圍內的封包及封包 Meta 資料資訊。

限制：這些搜尋僅限診斷之用途。 需要執行手動清理，以避免填滿擷取分割區。

程序

1. 按一下**搜尋**頁面。

   預設值已輸入。
2. 選取要搜尋其擷取資料流量的接口。

   如果您有單個接口配置，則會自動選取它。
3. 指定要搜尋之時間範圍的開始與結束時間值或變更預設值。
4. 指定「Berkeley 封包過濾器 (BPF)」。

   使用 BPF 語法來指定 BPF 過濾器。 表示式由一或多個基本元素組成。 複式過濾表示式可使用 AND、OR 與 NOT 運算子來建置。

   下列範例為基本過濾器

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   下列範例為複式過濾器

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. 指定要擷取的封包數。

   要擷取的預設封包數上限為 10,000。 如果將該數字變更為 0，則會擷取符合時間表及過濾器的所有封包。
6. 按一下**開始搜尋**。
7. 在搜尋頁面的**動作**直欄中，使用**分割區塊**選項來將搜尋要求分割為較小的資料區段，以便您可以在整個搜尋要求仍在執行中時存取資料。您可以首先透過指定 PCAP 檔案號碼，然後按一下**下載 PCAP 檔案**，來要求搜尋。

資料區段是 128 MB，而最新的資料區段可以是小於 128 MB 的任意大小。

8. 若要查看搜尋佇列的狀態，請檢視**搜尋要求佇列**。
9. 若要查看所有已完成搜尋的歷程，請檢視**要求日誌**。
10. 手動清除搜尋，以確保有足夠空間來用於 Forensics 回復處理：
    a. 以 root 使用者身分登入。

       使用者名稱：root

       密碼：P@ck3t08..

    b. 執行下列指令：

       ```
       rm -r /extraction/<name_of_search>
       ```

       <name_of_search> 變數是「已完成的搜尋」頁面上的名稱欄。

第 7 章 配置前置擷取過濾器

前置擷取過濾器可在將擷取資料寫入磁碟之前過濾網路資料流量。

程序

1. 建立前置擷取過濾器。
   a. 按一下**前置擷取過濾器**功能表。
   b. 輸入「過濾器名稱」和「搜尋過濾器」選項的設定。

      擷取過濾器會採用由連結 (and/or) 和選擇性地由 not 置前連接的基本元素表示式組成。

      在下列範例中，已捨棄目的地為埠 80 的所有資料流量：

      ```
      not dst port 80
      ```

      在下列範例中，只擷取這兩個主機的資料流量，並捨棄其他所有資料流量：

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```
   c. 按一下**新增**以完成前置擷取過濾器。 前一個新增至清單的前置擷取過濾器為作用中的過濾器。前一個過濾器的歷程也將顯示。
2. 重新啟動擷取程式伺服器，以啟動新增的過濾器。
3. 選取**刪除**來永久地刪除過濾器。您必須重新啟動擷取程式伺服器。

第 8 章 配置作用中的觸發程式

作用中的觸發程式可在您網路上發生指定事件時給出警示。例如，您可以指定 IP 位址作為搜尋過濾器，以當資料流量包含擷取的 IP 位址時給出警示。

程序

1. 建立作用中的觸發程式。
   a. 按一下**作用中的觸發程式**功能表。
   b. 輸入「觸發程式名稱」和「時間範圍」選項的設定。
   c. 按一下**新增**以完成作用中的觸發程式。

      限制：您可以最多指定五個作用中的觸發程式。
2. 發生觸發事件時，在**事件日誌**中檢查這些事件。按一下作用中的觸發事件，以在觸發事件的指定時間參數內自動產生搜尋要求。搜尋時間包括事件之前和之後的秒數。
3. 選取**刪除**來刪除配置的觸發程式。

第 9 章 QRadar Packet Capture 問題疑難排解

疑難排解是解決問題的系統方法。 疑難排解的目標是判斷為何有些功能未按預期工作，以及說明如何解決問題。

是否已安裝最新版本的 QRadar Packet Capture 軟體？

一律升級至軟體的最新發行版本。在套用軟體更新項目之後，或者在任何新的安裝之後，確保您立即重新啟動系統，從而套用變更。在叢集配置中，一律確保主要與所有資料節點系統都升級至相同版本。

您有 RAID 控制器及硬碟的建議韌體嗎？

如果您有 3650 M4 RAID 控制器及硬碟上安裝之韌體版本的相同可靠性或效能問題，請確保您有最低韌體修訂：

- 對於 3650 M4，M5200 RAID 控制器韌體修訂：2015 年 5 月 27 日 24.7.0-0052 版或更新版本。

  從 Red Hat Linux 指令行上執行 `.bin` 檔。
- 對於 IBM Lenovo，2015 年 5 月 15 日修訂或更新版本。

  從 Red Hat Linux 指令行上執行 `.bin` 檔。

在 BIOS 中是否已啟用 HyperThreading？

依預設，會在 BIOS 中啟用 HyperThreading。執行 `lscpu` 指令並檢查輸出，以確保「每個核心的執行緒數目等於 2」。下面是 IBM 3650-M4 的指令輸出範例：

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

是否已正確連接擷取埠？

IBM Security QRadar Packet Capture 裝置只能在 Interface 0 上擷取。

是否已正確配置乙太網路的網路連線？

若要確保已經為乙太網路介面指派 IP 位址，請針對已連接的介面執行 `ifconfig` 指令。

如果未配置任何位址，請編輯對應的 `ifcfg-eth*` 檔案以配置位址。

- 在此 DHCP 範例中，編輯 `/etc/sysconfig/network-scripts/ifcfg-eth2` 中的下列設定並使用適當的設定更換 *eth2*。

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- 在此靜態 IP 位址範例中，編輯 `/etc/sysconfig/network-scripts/ifcfg-eth2` 中的下列設定並使用適當的設定更換 *eth2*。

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  IPADDR="192.168.1.1"
  NETMASK="255.255.255.0"
  NM_CONTROLLED="no"
  ONBOOT="yes
  ```

變更設定之後，執行 `ifconfig` 指令以配置網路介面。

是否已正確配置系統時間？

依預設，系統時間設定為世界標準時間 (UTC)，並且配置為使用網路時間通訊協定 (NTP) 及公用伺服器正來保持正確的系統時間。

系統硬體是否有問題？

1. 確保資料流量得以正確產生並且由網路介面卡 (NIC) 接收。

   查看緊挨著介面 0 連線位於其右側的指示燈。 最下面的指示燈（表示鏈結）必須長亮。 最上面的指示燈（表示資料流量活動）必須閃爍。

2. 執行 /usr/local/nc/bin/dpdk_nic_bind.py –status 指令。

   指令的結果必須類似於下列輸出：

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

系統是否擷取資料流量？

在啟動擷取階段作業之後，若要確認系統是否正在擷取資料流量，請使用下列其中一種方法：

- 查看緊挨著介面 0 連線位於其右側的指示燈。 最上面的指示燈（表示資料流量活動）必須閃爍。
- 從「網路特性」頁面中，您可以看到圖形輸出。
- 從指令行中，執行 du –h /storage0/int0 指令。

  結果類似於下列輸出：

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

  如果您反覆地執行此指令，則傳回的子目錄和配置量數目將會遞增。

是否已啟用 QRadar Packet Capture Data Node？

當 QRadar Packet Capture Data Node 實際上連接到主要節點時，您還必須確保已在使用者介面中啟用它才能與主要伺服器搭配使用。系統目前最多支援兩個 QRadar Packet Capture Data Node。

如果**叢集**標籤顯示 QRadar Packet Capture Data Node 已連接且已啟用，並且**系統 ID** 設定從**更新節點 (n) 授權**畫面中**管理**標籤下遺漏，則必須確保特定 QRadar Packet Capture Data Node 與安裝為主要節點的 QRadar Packet Capture Data Node 的軟體版本相同。在更新到最新軟體版本之後，請確保符合此需求。

以 root 使用者的身分，執行下列指令以檢查 QRadar Packet Capture Data Node 和主要節點上安裝的軟體版本。

```
cat /root/version.txt
```

QRadar Packet Capture Data Node 軟體版本必須與主要節點上安裝的軟體版本相同。

如何從指令行套用 QRadar Packet Capture Data Node 的授權？

若要確保您位於 QRadar Packet Capture Data Node 中，請以 root 使用者的身分，執行下列指令：

```
cat /root/version.txt
```

若要驗證您已連接至 QRadar Packet Capture Data Node，請查看 D 是否附加到版本號碼末尾，例如 7.2.7.256D。

若要將授權套用至 QRadar Packet Capture Data Node，請以 root 使用者身分，執行以下 Script：nc_set_license.sh as root。

附註：

- 若要讓新授權生效，必須重新啟動 QRadar Packet Capture Data Node。
- 如果 QRadar Packet Capture Data Node 已在製造時授權，則不必執行該 Script。系統一旦啟動，授權便會生效。

如果您套用的授權無效，將會顯示錯誤訊息。

警告：LicenseKey *無效*.

LEEF 2.0 記載格式是甚麼？

LEEF（日誌事件延伸格式）訊息會採用以下格式新增到 /var/log/messages 檔案中：

```
<DateTime> <ServerIP> LEEF: 2.0|IBM|QRadar Packet Capture|7.2.7.256|<ID>|cat=<category> msg=<message>
```

例如，當 Packet Capture 伺服器在 IP 位址為 10.91.170.20 的系統上啟動時，會將以下 LEEF 訊息新增到 /var/log/messages 檔案：

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet Capture|7.2.7.256|Started|cat=PacketCapture
```

為何**建立搜尋**要求傳回 *NoSpace* 錯誤？

如果在您建立搜尋時 /extraction 目錄已滿，則伺服器會傳回 NoSpace 錯誤。

搜尋暫停時會發生甚麼情況？

當 /extraction 目錄中的已用的空間超過 6.7 GB 時，搜尋會暫停。會將一條 LEEF 訊息傳送至 Syslog，指示搜尋已暫停。事件日誌會顯示類似如下的警告：

```
!WARNING: Extraction Storage Full! Search cannot proceed!!
```

若要確保回復暫停的搜尋，必須透過刪除先前完成的較舊搜尋騰出空間。若要刪除舊的搜尋，請遵循下列步驟：

1. 按一下**搜尋**主功能表選項。
2. 在**搜尋要求日誌**頁框中，透過按一下**刪除搜尋**來刪除較舊的搜尋。

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 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）。

Printed in Taiwan