排除ESA和SMA上的集中PVO隔離故障

目錄

簡介

本文檔介紹如何在啟用集中策略、病毒和爆發隔離時排除傳輸和連線問題。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用AsyncOS 8.1或更新版本的電子郵件安全裝置(ESA)
- 採用AsyncOS 8.0或更高版本的安全管理裝置(SMA)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

集中策略、病毒和爆發(PVO)隔離區功能是在AsyncOS 8.0(ESA)/8.1(SMA)中引入的。 此功能具有額外的網路連線要求，並且給故障排除帶來了一些新的挑戰。

瞭解通訊

- CPQ通訊使用SMTP，但是使用一些額外的命令傳輸後設資料
- SMA將偵聽在Centralized Services -> Policy， Virus and Outbreak Quarantines下定義的介面和埠上的連線。 預設情況下，埠為7025，但管理員使用者可能已更改了該埠！
- ESA將偵聽在Security Services -> Policy， Virus and Outbreak Quarantines下定義的介面和埠上的連線。 同樣，預設情況下，埠為7025，但管理員使用者可能已更改了該埠！
- SMA還使用SSH（通過命令客戶端）從ESA獲取配置資訊。 具體來說，當SMA將已發佈的電子郵件傳送到ESA時使用。 SMA將使用SSH來查詢ESA配置，並確定要將已發佈電子郵件傳送到的介面/埠。

偵聽程式

- ESA和SMA都將有一個名為「cpq_listener」的隱藏監聽程式，該監聽程式將在指定的埠監聽。
- 可在配置檔案中看到這些監聽器。 例如：

```
<listener>
     <listener_name>cpq_listener</listener_name>
     <protocol>CPQ</protocol>
     <interface_name>Incoming Mail</interface_name>
     <port>7025</port>
     <listen_queue_size>50</listen_queue_size>
     <type>private</type>
     <hat>
$RELAYED
   RELAY {}
$BLOCKED
   REJECT {}
RELAYLIST:
   10.1.2.3
       $RELAYED (Only select hosts can relay from this box)
ALL
   $BLOCKED (Everyone else)
     </hat>
     <rat>
       <rat_entry>
         <rat_address>ALL</rat_address>
         <access>ACCEPT</access>
       </rat_entry>
     </rat>
```

- 如果管理員使用者使用「suspendlisteners all」或「suspend」，則這些偵聽程式將掛起。 如果埠不接受連線，則應檢查系統狀態是否為「離線」，如果需要，應恢復連線。

排除從ESA到SMA的交付故障

- 檢查ESA是否可以在配置的埠和介面上連線到SMA。 可以使用telnet完成。 如果通訊成功，您應該獲得220條標語。
- ESA將有一個名為「the.cpq.host」的目標對象，其中包含排隊等待傳遞到SMA的消息。 可以使用「tophosts」或「Monitor ->傳送狀態」檢視此資訊。 不能將「hoststatus」與其一起使用，但必要時可以使用「show recipients」和「deleterecipients」。

排除從SMA到ESA的交付故障

- 檢查SMA是否可以在配置的埠和介面上連線到ESA。 同樣地，您可以使用telnet，如果成功，您將看到220標語。
- 使用集群時，必須在集群級別的安全服務 — >策略、病毒和爆發隔離區下定義的介面存在於機器級別的所有裝置。 （檢查Network -> IP Interfaces）。
- SMA將有一個名為「the.cpq.release.host」的目標對象，該對象包含排隊等待傳遞到ESA的已釋放消息。 可以使用「tophosts」檢視此資訊。 這似乎不適用於「hoststatus」或「showrecipients」，我也未使用它測試「deleterecipients」，但這可能也不適用。
- SMA和ESA之間的SSH通訊也可能出現問題。 這些問題並非總是基於網路，例如，在CSCus29647中，SMA的內部元件無法運行。 此類問題通常會在郵件日誌中顯示為應用程式故障，通常可以通過重新啟動SMA來解決。

TLS/證書

- 任一方向的所有CPQ連線都依賴TLS，因此密碼配置可以發揮作用。
- 要使TLS連線成功，開啟連線的裝置必須能夠驗證接收裝置是否使用了我們的隱藏CPQ證書。 如果裝置協商匿名密碼，此操作可能會失敗。 日誌中將顯示如下內容：

```
Mon Apr  1 12:00:00 2014 Info: New SMTP DCID 123456 interface 10.0.0.2 address 10.0.0.1 port
7025
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS failed: verify error: no certificate from
server
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS was required but could not be successfully
negotiated
```

- 您只需從傳出傳遞密碼清單中刪除匿名密碼即可解決這些問題，方法是將「:-aNULL」新增到密碼清單末尾。 例如：高：中： **— 空**

日誌檔案

- 如果SMA訂用郵件日誌（預設情況下訂用），您可以檢視郵件日誌以收集其他資訊。
- 對於隔離到SMA的郵件和釋放到ESA的郵件，CPQ接收事件將如下所示

```
New CPQ ICID 12345 interface Management (10.10.10.1) address 10.10.20.1 reverse dns host
unknown verified no
```

- 您可以使用grep搜尋這些事件，例如：grep "CPQ ICID" mail_logs
- 從ESA隔離和從SMA隔離的CPQ傳送事件看起來與其他任何傳送類似，但列出了自定義埠，並且有幾行包含「集中策略隔離」的措辭。 以下示例：

```
Fri Sep 13 15:08:02 2013 Info: New SMTP DCID 12345 interface 10.10.20.1 address 10.10.10.1
port 7025
Fri Sep 13 15:08:02 2013 Info: DCID 12345 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Fri Sep 13 15:08:02 2013 Info: Delivery start DCID 12345 MID 23456 to RID [0] to Centralized
Policy Quarantine
Fri Sep 13 15:08:02 2013 Info: Message done DCID 12345 MID 23456 to RID [0] (centralized
policy quarantine)
Fri Sep 13 15:08:07 2013 Info: DCID 12345 close
```

- 您可以使用grep搜尋連線埠來尋找這些事件，例如：grep "port 7025" mail_logs

已禁用ESA「啟用」按鈕

嘗試在ESA上啟用PVO時，您可能會發現「啟用」按鈕呈灰色顯示，儘管所有前提條件配置都已完成。當ESA顯示PVO頁面時，它會通過埠7025與SMA進行通訊，以驗證配置是否已準備啟用。 如果此通訊失敗，將禁用「啟用」按鈕。 您可以像對任何ESA -> SMA埠7025通訊一樣對ESA上的「埠7025」進行故障排除。有關詳細資訊，請參閱「相關資訊」中列出的TechNote。

相關資訊

- [ESA群集時PVO遷移嚮導的要求]
- [無法啟用ESA集中策略、病毒和爆發隔離(PVO)]