ASA故障排除指南：系統日誌目標中缺少日誌

目錄

簡介

本文描述如何利用自適應安全裝置(ASA)將系統日誌傳送到各種目標的功能來排除故障，更具體地說，是發現以下症狀的問題：

- 自適應安全裝置管理器(ASDM)上的即時記錄速度緩慢。
- 一個或多個系統日誌目標上缺少間歇性系統日誌。

開始之前

需求

本文件沒有特定需求。

採用元件

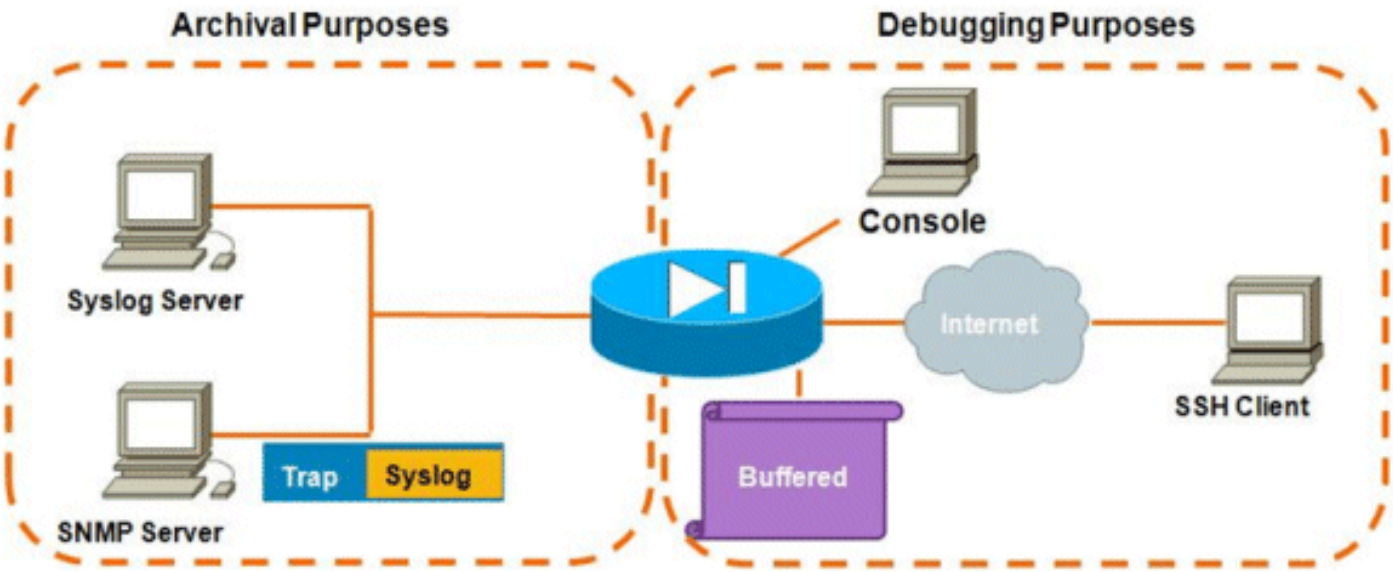
本文檔中的資訊基於Cisco ASA，並不限於特定ASA軟體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

功能資訊

ASA與大多數其他思科裝置一樣，能夠向多個系統日誌目標傳送系統日誌。下面列出了一些較常用的目標：



可能的目的地數目是一個真正的優勢。如果經過仔細選擇（如本文所示），它們可以根據其所服務的目的大致分為兩大類：

- 存檔
- 即時調試/故障排除

在大多數網路中，僅啟用歸檔目標就足夠了，除非需要一個或多個調試目標。同時，在較高的日誌級別（如資訊級別6或以上）同時啟用多個系統日誌目標時，經常會出現問題。

故障排除方法

每當在一個或多個目的地丟失系統日誌資訊時出現問題時，您應該檢查以下兩點：

- 檢視系統日誌記錄配置(show run logging的輸出)。
- 檢視show logging queue的輸出。

資料分析

檢視系統日誌配置

請完成以下步驟：

1. 確保您查詢的系統日誌消息沒有被no logging message *<ID>*命令禁用。
2. 確認後，檢視已啟用系統日誌目標的數量以及每個日誌傳送到每個目標的級別。以下是此類組態範例：

```
logging enable
logging timestamp
logging standby
logging console informational
logging buffered informational
logging trap informational
logging asdm informational
logging device-id hostname
logging host inside 172.16.110.32
```

在此示例中，ASA正在將系統日誌傳送到資訊級別（級別6）的4個不同目標。

show logging queue的輸出

使用上述配置（多個目標接收大量日誌消息），可能會出現ASA由於日誌隊列溢位而丟棄系統日誌消息的情況。在這種情況下，輸出將如下所示：

```
ciscoasa# show logging queue

   Logging Queue length limit : 512 msg(s)
   2352325 msg(s) discarded due to queue overflow
   0 msg(s) discarded due to memory allocation failure
   Current 512 msg on queue, 512 msgs most on queue
```

預設情況下，日誌記錄隊列容納512條消息。

常見問題

如果遇到系統日誌消息未記錄的問題，請考慮以下選項：

- 禁用控制檯日誌記錄。不應為正常操作**啟用**登入到控制檯。控制檯日誌記錄應僅用於即時故障排除，日誌記錄級別低或流量低。以高速率登入到控制檯將導致日誌記錄過程嚴重限制消息的速率。控制檯只能以9600 bps的速度記錄消息，並且在開始嘗試向控制檯轉儲超過控制檯輸出到螢幕的容量之前不會佔用大量日誌。在這種情況下，日誌將開始緩衝在日誌記錄隊列中。日誌記錄隊列填滿後，消息將被尾部丟棄。
- 將**日誌記錄隊列大小增加**到512以上。ASA-5505上的最大日誌記錄隊列為1024,ASA-5510上的最大日誌記錄隊列為2048，所有其他平台上的最大日誌記錄隊列為8192。附註：日誌記錄隊列用於「突發」系統日誌。如果syslog的持續速率比ASA可以將它們傳輸到各種目的地的速度快，則日誌記錄隊列限制將不夠大。
- 禁用您對存檔不感興趣的單個系統日誌消息。發出no logging message *<syslog_id>* 命令以停用個別系統日誌。
- 請注意將消息記錄到ASA的磁碟（快閃記憶體）。寫入快閃記憶體的操作非常緩慢。過多記錄到快閃記憶體會導致ASA將系統日誌檔案緩衝在記憶體中，最終耗盡所有可用記憶體(RAM)。此外，將大量系統日誌消息記錄到快閃記憶體可能會提高CPU。建議僅將級別1的消息記錄到快閃記憶體（涵蓋關鍵系統事件）。

相關資訊

- 技術支援與文件 - Cisco Systems