自適應安全裝置上的日誌和調試之間的差異

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[基本日誌功能](#)
[系統日誌和調試消息之間的差異](#)
[收集調試](#)
[示例配置](#)
[相關資訊](#)

簡介

本文檔對運行8.4及更高版本的自適應安全裝置(ASA)中的調試功能進行了簡單說明。但是，某些功能僅在9.5(2)版及更高版本中可用。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 具備ASA軟體版本9.5(2)的ASA 5506-X
- 思科調適型安全裝置管理員(ASDM)版本7.5.2

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。

基本日誌功能

ASA處理調試消息的方式與Cisco IOS®裝置不同。預設情況下（除非使用後面介紹的「logging debug-trace」），它們會在您通過控制檯埠連線或通過telnet/Secure Shell(SSH)連線時在螢幕上顯示，但它們完全獨立。使用控制檯時，在輸入debug命令後會立即顯示它們。SSH會話也會發生同樣的操作。

獨立表示當您在控制檯埠上啟用調試並且通過SSH連線時，調試不會顯示在SSH上。您必須再次手動啟用它們。此外，如果在一個SSH會話上啟用調試，它們將不會顯示在另一個會話上。您可以根據作業階段偵**錯參考該檔案。**

此外，無需在ASA上輸入**terminal monitor**命令即可顯示調試，因為無論此命令如何，在SSH或telnet會話上啟用的調試都會顯示。此命令的用途與Cisco IOS裝置中的用途有很大不同，而ASA系統日誌配置示例將深入介紹此功能。

系統日誌和調試消息之間的差異

調試是為ASA的特定協定或功能指定的消息。沒有調試級別，而是非常詳細，可以更改詳細級別。它們也可能沒有時間戳、消息代碼或嚴重性級別。這取決於特定的偵錯。

此範例顯示相同ping要求方面的偵錯和系統日誌訊息之間的差異。

以下是輸入**debug icmp trace** 指令後的偵錯輸出範例：

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

以下是有關同一ICMP要求的**syslog**訊息範例：

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

收集調試

SSH或telnet的預設超時為5分鐘，在此時間不活動後會話將斷開。控制檯連線的預設超時為0，這意味著使用者登入直到使用者手動註銷。

遺憾的是，日誌記錄功能受到特定管理方法上設定的超時的限制，因此，當SSH會話結束時，調試也會停止。

若要在更長的時間內繼續收集調試，必須使用控制檯連線，然後使用**logging debug-trace** 命令將它們重定向到系統日誌伺服器。它們將被重定向為在嚴重性級別7發出系統日誌消息711001。為了停止向日誌傳送此消息，您可以在命令前插入「no」。

```
logging debug-trace
no logging debug-trace
```

從9.5.2版本開始，ASA允許您在超時後繼續以系統日誌消息的形式傳送調試，或在SSH/telnet/控制檯連線上註銷。如果您輸入**debug-trace persistent**命令，則可以從另一個會話選擇性地清除一個會話中啟用的調試，這些調試在後台將保持活動狀態。若要停用此功能，請在命令前插入「no」。

```
logging debug-trace persistent
no logging debug-trace persistent
```

預設情況下，所有調試消息的嚴重性都為7級。為了從不需要的消息中過濾這些消息，您可以將此消息的嚴重性提高至3，以便只收集調試消息旁邊的錯誤消息。插入「no」以停用此重新導向。

```
logging message 711001 level 3
```

```
no logging message 711001 level 3
```

示例配置

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

這些命令可讓您向系統日誌伺服器傳送錯誤消息和標記為錯誤的網際網路控制消息協定(ICMP)調試：

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

相關資訊

- ASA系統日誌配置示例
- 技術支援與文件 - Cisco Systems