FWSM故障轉移故障排除

目錄

簡介

本檔案將說明可用於解決防火牆服務模組(FWSM)容錯移轉組態問題的程式。

本文檔還提供了常見過程的清單，在您開始排除故障切換連線故障之前需要嘗試這些步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據FWSM 2.3及更新版本。

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

故障切換功能允許備用FWSM接管故障的FWSM的功能。所涉及的兩個FWSM必須具有相同的主要（第一個數字）和次要（第二個數字）軟體版本、許可證和操作模式（路由或透明、單個或多個情景）。 當主用裝置發生故障時，狀態變為備用，而備用裝置進入主用狀態。發生故障切換後，新的主用裝置會提供相同的連線資訊。

有關其他資訊，請參閱使用故障切換的配置故障切換部分。

故障轉移核對清單

此核對清單可幫助您在FWSM中成功配置故障轉移：

- 檢驗介面
- 授權
- 上下文模式
- 軟體需求
- 狀態故障切換的最小FWSM配置
- 最小交換機配置

檢驗介面

驗證FWSM上的所有介面都配置了備用IP地址。如果尚未進行配置，請為每個介面（路由模式）或管理地址（透明模式）配置主用和備用IP地址。 備用IP地址用於當前作為備用裝置的FWSM。它必須與活動IP地址位於同一個子網中。

以下是組態範例：

```
ip address <active-ip> <netmask> standby <standby-ip>
```

注意：請勿為故障切換鏈路或狀態鏈路配置IP地址（如果要使用狀態故障切換）。

注意：您不需要標識備用地址子網掩碼。故障切換時故障切換鏈路IP地址和MAC地址不會更改。故障切換鏈路的主用IP地址始終位於主裝置上，而備用IP地址始終位於輔助裝置上。

授權

主用和備用裝置必須具有相同的許可證。

上下文模式

如果主裝置處於單情景模式，則輔助裝置還必須處於單情景模式，並且與主裝置處於相同的防火牆模式。

如果主裝置處於多情景模式，則輔助裝置也必須處於多情景模式。您不需要在輔助裝置上配置安全上下文的防火牆模式，因為故障切換和狀態鏈路位於系統上下文中。輔助單元從主單元獲取安全上下文配置。

註：mode命令不會複製到輔助裝置。

注意：安全裝置的多情景模式不支援組播。有關詳細資訊，請參閱不支援的功能部分。

軟體需求

故障切換配置中的兩個裝置必須具有相同的主要（第一個數字）和次要（第二個數字）軟體版本。但是，您可以在升級過程中使用不同版本的軟體。例如，您可以將一個裝置從3.1(1)版升級到3.1(2)版，並使故障切換保持活動狀態。思科建議將兩台裝置升級到相同版本以確保長期相容性。

狀態故障切換的最小FWSM配置

主FWSM

```
failover lan unit primary
failover lan interface if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr failover link if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr
```

輔助FWSM

```
failover lan unit secondary
failover lan interface if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr failover link if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr
```

有關如何配置主用和備用故障切換的詳細資訊，請參閱配置主用/備用故障切換。

最小交換機配置

- 包含主節點的Catalyst傳送到主FWSM的VLAN必須與包含次節點的Catalyst傳送到輔助FWSM的VLAN匹配。(show run**的輸出 | i**防火牆命令必須相同。)**主機箱**

  ```
  cat6k-7(config)#do sh run | i fire
  firewall multiple-vlan-interfaces
  firewall module 9 vlan-group 1
  firewall vlan-group 1  3,4,100-106
  ```

  輔助機箱

  ```
  cat6k-7(config)#do sh run | i fire
  firewall multiple-vlan-interfaces
  firewall module 9 vlan-group 1
  firewall vlan-group 1  3,4,100-106
  ```

- 傳送的所有VLAN必須存在於VLAN資料庫中並且處於活動狀態。若要執行此操作，請在設定模式下交換器上發出以下命令：

  ```
  vlan 10
  no shut
  ```

若要確認VLAN是否位於資料庫中且處於作用中狀態，兩個機箱上的**show vlan**命令輸出必須包含傳送到FWSM的VLAN並顯示為作用中狀態。以下是輸出範例：**主機箱**

```
cat6k-7(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----
1    default                               active
3    VLAN0003                         active    Fa4/47
4    VLAN0004                         active    Fa4/48
```

輔助機箱

```
cat6k-7(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----
1    default                               active
3    VLAN0003                         active    Fa4/47
4    VLAN0004                         active    Fa4/48
```

- 確保兩個FWSM在每個VLAN中具有第2層連線（它們必須位於同一個子網中）。**透明防火牆要求：**為了在透明模式下使用故障切換時避免環路，必須使用支援橋接協定資料單元(BPDU)轉發的交換機軟體。此外，您必須將FWSM配置為允許BPDU。為了允許BPDU通過FWSM，請配置EtherType?ACL並將其應用於兩個介面。**注意：**與PIX和ASA平台相反，兩個FWSM刀片的硬體始終相同，沒有不同的型號或記憶體配置。

疑難排解

當FWSM重新載入時，本節介紹的場景將導致禁用故障切換。

FWSM可以因以下原因重新載入：崩潰、從機箱重置、從FWSM CLI發出重新載入，或者它可以是插入或重新拔插到其他插槽或從機箱重新通電的新模組。

版本不匹配

故障切換配置中的兩個裝置必須具有相同的主要（第一個數字）和次要（第二個數字）軟體版本。

相關系統日誌消息：105040

不相容的許可證

由於許可證不相容，您可能會收到此系統日誌：

```
FWSM-1-105045: (Primary) Mate license (number contexts) is not compatible
with my license (number contexts).
FWSM-1-105001: (Primary) Disabling failover.
```

相關系統日誌消息：105045和105001

不同模式（單情景和多情景）

主FWSM和輔助FWSM必須處於同一模式（單個或多個）。 例如，如果主模組配置為單模式，輔助模組配置為多模式，並且輔助模組重新載入，則兩個模組都將關閉故障切換。

單模式下的主模式：

```
%FWSM-1-103001: (Primary) No response from other firewall (reason code = 1).
%FWSM-1-105044: (Primary) Mate operational mode (Multi) is not compatible
with my mode (Single).
%FWSM-1-105001: (Primary) Disabling failover.
```

多模式下的輔助模式（此刀片已重新載入）：

```
%FWSM-5-111008: User 'Config' executed the 'no snmp-server location' command.
%FWSM-5-111008: User 'Config' executed the 'inspect tftp' command.
%FWSM-5-111008: User 'Config' executed the 'service-policy global_policy global'
command.
%FWSM-5-111008: User 'Config' executed the 'config-url disk:/admin.cfg' command.
%FWSM-5-111008: User 'Config' executed the 'prompt hostname context' command.
%FWSM-4-411001: Line protocol on Interface LAN, changed state to up
%FWSM-4-411001: Line protocol on Interface LAN, changed state to up
%FWSM-1-105044: (Secondary) Mate operational mode (Single) is not compatible
with my mode (Multi).
%FWSM-1-105001: (Secondary) Disabling failover.
%FWSM-6-199002: Startup completed.  Beginning operation.
%FWSM-6-605005: Login permitted from 127.0.0.51/15518 to eobc:127.0.0.91/telnet
for user ""
%FWSM-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
%FWSM-5-111008: User 'enable_15' executed the 'changeto context admin' command.
```

多模式下的主模式：

```
%FWSM-1-105044: (Primary) Mate operational mode (Single) is not compatible
with my mode (Multi).
%FWSM-1-105001: (Primary) Disabling failover.
```

相關系統日誌消息：105044、103001、105001

兩個FWSM變為活動狀態

當您在日誌中看到以下錯誤消息時：

```
fw_create_pc_sw: fw_create_portchannel failed
```

此錯誤是因為交換器中的建議連線埠通道數超過最大值(Cat6000/6500上的Cisco IOS軟體版本12.2(33)SXH4中的128是最大值)。 因此，介面描述符塊(IDB)限制已用盡。

因此，您可能會遇到以下兩個問題：

- 如果您有兩台具有FWSM模組的交換機，其中每台都用作主用和備用模組，則兩個FWSM模組將同時變為主用狀態。
- 無法建立附加的port-channel。

作為解決問題的一部分，請刪除不需要的埠通道並重新載入FWSM。

VLAN不匹配

問題

FWSM收到以下錯誤消息：**'Detected an Active Mate' 'Vlan configuration mismatch' 'failover will be disabled'**。

或

防火牆服務模組的配置和相應的交換機配置似乎已完成。但是，FWSM無法彼此同步。在輔助主機上收到了以下消息：

```
State check detected an Active mate

        Unable to verify vlan configuration with mate.
        Check that mate's failover is enabled

        No Response from Mate
```

或

show failover命令的輸出顯示，輔助模組上的故障切換狀態為OFF,FWSM故障切換狀態為Failover Off。

```
FWSM-secondary(config)#show failover
Failover Off (pseudo-Standby)
```

解決方案

問題可能是防火牆上的VLAN分配不匹配（FWSM和Supervisor）。 例如，在Firewall vlan-group 1語句中，每台交換機上分配給防火牆的相同VLAN數可能會有所不同。這可能會導致問題。如果在防火牆中分配的VLAN數量相同，則故障切換將起作用。

為了避免出現VLAN組態不相符錯誤，兩個FWSM上的**show vlan**指令輸出必須相同。只有在FWSM上修改或載入故障切換配置時，才會出現此錯誤消息。例如，當FWSM啟動時，它會從快閃記憶體載入啟動配置並嘗試初始化故障切換。此時，它會進行檢查以確保兩個模組都接收到正確的VLAN。如果VLAN不匹配，則會顯示錯誤消息，並且故障切換保持禁用狀態。

注意：為了故障切換正常工作，FWSM需要相同的配置和埠分配。機箱間故障轉移是可能的，但分配給防火牆的每個VLAN都必須位於兩個機箱之間的中繼線中。

FWSM不包括任何外部物理介面。相反，它使用VLAN介面。為FWSM分配VLAN類似於為交換機埠分配VLAN。FWSM包括一個到交換機交換矩陣模組（如果有）或共用匯流排的內部介面。如需詳細資訊，請參閱將VLAN指派給防火牆服務模組。

請注意，VLAN對映可以在正常運行的FWSM設定期間修改，並且將在下次引導時失敗。

已禁用故障轉移

使用no failover 命令禁用故障切換時，裝置的當前狀態（無論是活動還是備用）將一直保持到裝置重新載入。這僅用於禁用故障轉移。若要將裝置的狀態從活動更改為備用，反之亦然，您需要使用[no] failover active命令。

相關資訊

- FWSM:配置故障轉移
- FWSM:系統日誌消息
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。