# 目录



## 简介

本文档介绍用于解决防火墙服务模块 (FWSM) 故障切换配置问题的过程。

本文档还提供一个常规过程清单，以供在开始解决故障切换连接问题前尝试使用。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息根据FWSM 2.3及以上版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 背景信息

故障切换功能允许备用 FWSM 取代出现故障的 FWSM 的功能。相关的两个 FWSM 必须具有相同的主软件版本（第一个数字）和次软件版本（第二个数字）、许可证和操作模式（路由或透明，单上下文或多上下文）。当活动单元发生故障时，其状态将变为备用，同时备用单元将变为活动状态。在发生故障切换之后，新的活动单元具有相同的连接信息。

有关其他信息，请参阅“使用故障切换”的配置故障切换部分。

# 故障切换清单

以下清单将帮助您在 FWSM 中成功配置故障切换：

- 验证接口
- 许可证
- 上下文模式
- 软件要求
- 有状态故障切换的最小 FWSM 配置
- 最小交换机配置

## 验证接口

验证 FWSM 上的所有接口都具有一个已配置的备用 IP 地址。如果尚未配置，请为每个接口（路由模式）或管理地址（透明模式）配置活动和备用 IP 地址。备用 IP 地址用于当前作为备用单元的 FWSM 上。它必须与活动 IP 地址处于同一子网中。

以下是一个配置示例：

**注意：** 请勿配置故障切换链路或有状态链路的 IP 地址（如果您计划使用有状态故障切换）。

**注意：** 您不需要识别备用地址子网掩码。在发生故障切换时，故障切换链路 IP 地址和 MAC 地址不会更改。故障切换链路的活动 IP 地址始终用于主要单元，而备用 IP 地址始终用于辅助单元。

## 许可证

活动单元和备用单元必须具有相同的许可证。

## 上下文模式

如果主要单元处于单上下文模式下，则辅助单元也必须处于单上下文模式下，并且与主要单元使用相同的防火墙模式。

如果主要单元处于多上下文模式下，则辅助单元也必须处于多上下文模式下。您不需要配置辅助单元的安全上下文的防火墙模式，因为故障切换链路和有状态链路均驻留在系统上下文中。辅助单元

将从主要单元中获得安全上下文配置。

**注意： 模式命令**不会被复制到辅助单元。

**注意：** 在安全设备的多上下文模式下不支持多播。有关详细信息，请参阅不支持的功能部分。

## 软件要求

在故障切换配置中，两个单元的主软件版本（第一个数字）和次软件版本（第二个数字）必须相同。但是，在升级过程中，您可以使用不同的软件版本。例如，您可以将一个单元的版本从 3.1(1) 升级到 3.1(2) 并使故障切换保持活动状态。Cisco 建议您将两个单元都升级为同一版本以确保长期兼容。

## 有状态故障切换的最小 FWSM 配置

**主要 FWSM**

**辅助 FWSM**

有关如何配置活动和备用故障切换的详细信息，请参阅配置活动/备用故障切换。

## 最小交换机配置

- 由 Catalyst 发送到主要 FWSM 的包含主要单元的 VLAN 必须与 Catalyst 发送到辅助 FWSM 的包含辅助单元的 VLAN 匹配。（**show run|** 命令的输出必须相同。）**主要机箱**`cat6k-7(config)#do sh run | i fire firewall multiple-vlan-interfacesfirewall module 9 vlan-group 1firewall vlan-group 1 3,4,100-106`**辅助机箱**`cat6k-7(config)#do sh run | i fire firewall multiple-vlan-interfacesfirewall module 9 vlan-group 1firewall vlan-group 1 3,4,100-106`
- 所有发送的 VLAN 必须存在于 VLAN 数据库中，并且处于活动状态。要执行此任务，请在配置模式下的交换机中发出以下命令：**vlan 10no shut**要验证 VLAN 是否位于数据库中并且处于活动状态，两个机箱的 **show VLAN** 命令输出都必须包含发送到 FWSM 的 VLAN，并且显示为活动状态。以下是输出示例：**主要机箱**`cat6k-7(config)#do sh vlanVLAN Name Status Ports---- -------------------------------- --------- -----1 default active 3 VLAN0003 active Fa4/474 VLAN0004 active Fa4/48`**辅助机箱**`cat6k-7(config)#do sh vlanVLAN Name Status Ports---- -------------------------------- --------- -----1 default active 3 VLAN0003 active Fa4/474 VLAN0004 active Fa4/48`
- 请确保两个 FWSM 的每个 VLAN 中都具有第二层连接（它们必须位于相同子网中）。**透明防火墙要求：**为了避免环路，当您在透明模式时使用故障切换，您必须使用交换机软件该支持网桥协议数据单元(BPDU)转发。并且，您必须配置 FWSM 以允许 BPDU。要允许 BPDU 通过 FWSM，请配置一种以太网类型？ACL，并将其应用于两个接口。**注意：** 与 PIX 和 ASA 平台相反，两个 FWSM 刀片的硬件始终是相同的，其型号或内存配置没有不同。

# 排除故障

当 FWSM 重新加载时，本部分中介绍的方案将造成故障切换被禁用。

在出现崩溃、从机箱中重置、从 FWSM CLI 中发出重新加载命令、在不同插槽中插入或重置新模块

，或者机箱重新连接电源时，FWSM 可以重新加载。

## 版本不匹配

在故障切换配置中，两个单元的主软件版本（第一个数字）和次软件版本（第二个数字）必须相同。

相关系统消息：105040

## 不兼容许可证

您可能会由于许可证不兼容而收到以下系统日志：

```
cat6k-7(config)#do sh vlanVLAN Name                             Status    Ports---- ------------
-------------------- --------- -----1    default                                  active    3
VLAN0003                         active    Fa4/474    VLAN0004                              active
Fa4/48
```

相关系统消息：105045和105001

## 不同模式（单上下文与多上下文）

主要 FWSM 和辅助 FWSM 必须处于相同模式下（单上下文或多上下文）。例如，如果主要 FWSM 配置为单模，而辅助 FWSM 配置为多模，则在辅助 FWSM 重新载入时，两个模块的故障切换都将关闭。

主要 FWSM 处于单模：

```
cat6k-7(config)#do sh vlanVLAN Name                             Status    Ports---- ------------
-------------------- --------- -----1    default                                  active    3
VLAN0003                         active    Fa4/474    VLAN0004                              active
Fa4/48
```

辅助 FWSM 处于多模（此刀片将被重新载入）：

```
cat6k-7(config)#do sh vlanVLAN Name                             Status    Ports---- ------------
-------------------- --------- -----1    default                                  active    3
VLAN0003                         active    Fa4/474    VLAN0004                              active
Fa4/48
```

主要 FWSM 处于多模：

```
cat6k-7(config)#do sh vlanVLAN Name                             Status    Ports---- ------------
-------------------- --------- -----1    default                                  active    3
VLAN0003                         active    Fa4/474    VLAN0004                              active
Fa4/48
```

相关系统消息：105044， 103001， 105001

## 两个 FWSM 变为活动状态

当您在日志中看到此错误消息时：

```
cat6k-7(config)#do sh vlanVLAN Name                             Status    Ports---- ------------
-------------------- --------- -----1    default                                  active    3
VLAN0003                         active    Fa4/474    VLAN0004                              active
Fa4/48
```

此错误的原因是，因为交换机中的建议端口通道数量超出了最大数量（在 Cat6000/6500 上的

Cisco IOS 软件版本 12.2(33)SXH4 中，最大数量为 128 ）。所以，接口描述符模块(IDB)限制用尽。

因此，您也许最终获得这两个问题：

- 当您具有两台交换机，每台交换机具有一个 FWSM 模块，并且其中一台交换机作为活动交换机，另一台交换机作为备用交换机时，这两个 FWSM 模块将同时变为活动状态。
- 您不能创建其他端口通道。

作为解决问题一部分，请删除不是需要的端口通道并且重新加载FWSMs。

## VLAN 不匹配

### 问题

FWSM 收到以下错误消息：**'Detected an Active Mate'** 'Vlan configuration mismatch' 'failover will be disabled'.

**或者**

防火墙服务模块的配置和相应的交换机配置似乎是完整的。但是，FWSM 之间无法相互同步。在辅助主机上收到了以下消息：

```
cat6k-7(config)#do sh vlanVLAN Name                                 Status    Ports---- ------------
-------------------- --------- -----1    default                                  active    3
VLAN0003                         active    Fa4/474    VLAN0004                                 active
Fa4/48
```

**或者**

**show failover** 命令输出显示，辅助模块的故障转移状态为关闭，FWSM 故障切换状态则是“故障切换关闭”(pseudo-Standby)。

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

### 解决方案

此问题可能是防火墙间的 VLAN 分配（FWSM 和 Supervisor）不匹配引起的。例如，在防火墙 VLAN 组 1 语句中，每台交换机上分配给防火墙的相同 VLAN 数量可能不同。这可能会导致问题。如果在防火墙中分配相同数量的 VLAN，则故障切换将正常工作。

为避免收到 VLAN 配置不匹配错误，两个 FWSM 上的 **show VLAN** 命令输出必须相同。仅当您在 FWSM 上修改或加载故障切换配置时，此错误消息才会出现。例如，当 FWSM 启动时，它将从闪存中装载启动配置，并尝试初始化故障切换。此时，它将进行检查以确定两个模块都收到正确的 VLAN。如果 VLAN 不匹配，则将显示错误消息，并且故障切换仍将保持禁用。

**注意：** 要启用故障切换，FWSM 要求使用相同的配置和端口分配。您可以在机箱间进行故障切换，但分配给防火墙的每个 VLAN 必须位于两个机箱之间的中继上。

FWSM 不包括任何外部物理接口。相反，它使用的是 VLAN 接口。将 VLAN 分配到 FWSM 与将 VLAN 分配到交换机端口类似。FWSM 包括到交换矩阵模块（如果存在）或共享总线的内部接口。有关详细信息，请参阅将 VLAN 分配到防火墙服务模块。

请注意，VLAN 映射可能在工作 FWSM 设置期间被修改，并在下一次引导时失败。

### 故障切换禁用

使用no failover命令时，当您禁用故障切换，单元的当前状态被保持(是否能起作用的或备用的)直到单元重新载入。这用于只禁用故障切换。为了更改单元的状态从激活到待机或反之亦然，您需要使用[no] failover active命令。

## 相关信息

- FWSM ：配置故障切换
- FWSM ：系统日志消息
- 技术支持和文档 - Cisco Systems