# Troubleshooting de Failover de FWSM

## Contents



# Introduction

Este documento explica os procedimentos que você pode usar para resolver problemas com a configuração de failover do módulo de serviço de firewall (FWSM).

Este documento também fornece uma lista de verificação de procedimentos comuns a serem tentados antes de você começar a solucionar problemas da conexão de failover.

# Prerequisites

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas no FWSM 2.3 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Informações de Apoio

O recurso de failover permite que um FWSM em standby assuma a funcionalidade de um FWSM com falha. Os dois FWSMs envolvidos devem ter a mesma versão de software principal (primeiro número) e secundária (segundo número), licença e modos de operação (roteado ou transparente, contexto único ou múltiplo). Quando a unidade ativa falha, o estado muda para standby, enquanto a unidade standby passa para o estado ativo. Após um failover, as mesmas informações de conexão ficam disponíveis na nova unidade ativa.

Para obter informações adicionais, consulte a seção Configuração de Failover de Uso de Failover.

## Lista de verificação de failover

Esta lista de verificação ajuda a configurar com êxito o failover no FWSM:

- Verifique as interfaces
- Licenças
- Modo de Contexto
- Requisitos de software
- Configuração mínima de FWSM para failover stateful
- Configuração mínima do switch

### Verifique as interfaces

Verifique se todas as interfaces no FWSM têm um endereço IP em espera configurado. Se ainda não tiver feito isso, configure os endereços IP ativo e standby para cada interface (modo roteado) ou para o endereço de gerenciamento (modo transparente). O endereço IP em standby é usado no FWSM que atualmente é a unidade em standby. Ele deve estar na mesma sub-rede do endereço IP ativo.

Este é um exemplo de configuração:

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

**Observação:** não configure um endereço IP para o link de failover ou para o link de estado (se for usar o failover stateful).

**Observação:** Você não precisa identificar a máscara de sub-rede do endereço em standby. Os

endereços IP e MAC do link de failover não são alterados no failover. O endereço IP ativo para o link de failover sempre permanece na unidade primária, enquanto o endereço IP em standby permanece na unidade secundária.

## Licenças

As unidades ativa e em espera devem ter a mesma licença.

## Modo de Contexto

Se a unidade primária estiver no modo de contexto único, a unidade secundária também deve estar no modo de contexto único e no mesmo modo de firewall que a unidade primária.

Se a unidade primária estiver no modo de contexto múltiplo, a unidade secundária também deve estar no modo de contexto múltiplo. Você não precisa configurar o modo de firewall dos contextos de segurança na unidade secundária porque os links de failover e de estado residem no contexto do sistema. A unidade secundária obtém a configuração do contexto de segurança da unidade primária.

**Nota:** O comando **mode** não é replicado para a unidade secundária.

**Observação:** o multicast não é suportado no modo de contexto múltiplo do Security Appliance. Consulte a seção Recursos sem Suporte para obter mais informações.

## Requisitos de software

As duas unidades em uma configuração de failover devem ter a mesma versão de software principal (primeiro número) e secundária (segundo número). No entanto, você pode usar versões diferentes do software durante um processo de atualização. Por exemplo, você pode atualizar uma unidade da versão 3.1(1) para a versão 3.1(2) e fazer com que o failover permaneça ativo. A Cisco recomenda atualizar ambas as unidades para a mesma versão para garantir a compatibilidade a longo prazo.

## Configuração mínima de FWSM para failover stateful

### FWSM primário

```
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
```

### FWSM secundário

```
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
```

Para obter mais informações sobre como configurar o failover ativo e em standby, consulte Configuração do Failover Ativo/em Standby.

## Configuração mínima do switch

- As VLANs enviadas ao FWSM primário pelo Catalyst que contém o primário devem corresponder às VLANs enviadas ao FWSM secundário pelo Catalyst que contém o secundário. (Saída do comando **show run | i** comando **firewall** deve ser idêntico.)**Chassi principal**

```
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
```

**Chassi secundário**

```
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
```

- Todas as VLANs enviadas devem estar presentes no banco de dados de VLANs e estar ativas.Para fazer isso, execute estes comandos no switch no modo de configuração:

```
vlan 10
no shut
```

Para verificar se as VLANs estão no banco de dados e ativas, a saída do comando **show vlan** em ambos os chassis deve conter as VLANs enviadas ao FWSM e mostradas como ativas.Esta é uma saída de exemplo:**Chassi principal**

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

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

**Chassi secundário**

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

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

- Certifique-se de que os dois FWSMs tenham conectividade de Camada 2 em cada VLAN (eles devem estar na mesma sub-rede).**Requisitos de firewall transparente:**Para evitar loops ao usar failover no modo transparente, você deve usar o software do switch que suporta o encaminhamento de BPDU (Bridge Protocol Data Unit). Além disso, você deve configurar o FWSM para permitir BPDUs. Para permitir BPDUs através do FWSM, configure um EtherType? ACL e aplique-a às duas interfaces.**Observação:** ao contrário da plataforma PIX e ASA, o hardware de dois blades FWSM é sempre o mesmo, não há modelos diferentes ou configurações de memória.

# Troubleshooting

Quando o FWSM for recarregado, os cenários explicados nesta seção farão com que o failover seja desabilitado.

O FWSM pode ser recarregado por motivos como travamento, reinicialização do chassi,

recarregamento emitido da CLI do FWSM ou pode ser apenas um novo módulo inserido ou recolocado em um slot diferente ou ligado novamente do chassi.

## Incompatibilidade de Versão

As duas unidades em uma configuração de failover devem ter a mesma versão de software principal (primeiro número) e secundária (segundo número).

Mensagem de syslog relacionada: 105040

## Licenças incompatíveis

Você pode receber este syslog devido a uma licença incompatível:

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

Mensagens de syslog relacionadas: 105045 e 105001

## Modos diferentes (contexto único versus contexto múltiplo)

O FWSM primário e secundário devem estar no mesmo modo (único ou múltiplo). Por exemplo, se o primário estiver configurado como modo único e o secundário como modo múltiplo e o secundário for recarregado, ambos os módulos desativarão o failover.

Primário em modo simples:

```
%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.
```

Secundário em modo múltiplo (este blade é recarregado):

```
%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.
```

Primário em modo múltiplo:

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

Mensagens de syslog relacionadas: 105044, 103001, 105001

## Dois FWSMs se tornam ativos

Quando você vir esta mensagem de erro no registro:

```
fw_create_pc_sw: fw_create_portchannel failed
```

A razão para esse erro é porque o número recomendado de port-channels no switch excedeu o máximo (128 é o máximo no Cisco IOS Software Release 12.2(33)SXH4 no Cat6000/6500). Portanto, o limite do Interface Descriptor Block (IDB) está sendo esgotado.

Por causa disso, você pode acabar tendo estes dois problemas:

- Quando você tem dois switches com módulos FWSM cada um para atuar como ativo e em espera, dois módulos FWSM se tornam ativos ao mesmo tempo.
- Não é possível criar um canal de porta adicional.

Como parte da resolução do problema, exclua os canais de porta que não são necessários e recarregue os FWSMs.

## Incompatibilidade de VLAN

### Problema

O FWSM recebe esta mensagem de erro: **'Foi detectada uma combinação ativa' 'Incompatibilidade de configuração de VLAN' 'o failover será desabilitado'**.

### OU

A configuração dos módulos de serviço de firewall e a configuração do switch correspondente parecem estar completas. No entanto, os FWSMs não podem sincronizar entre si. Esta mensagem é recebida no host secundário:

```
State check detected an Active mate

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

        No Response from Mate
```

### OU

A saída do comando **show failover** mostra que o status de failover no módulo secundário é `OFF`, estado de failover do FWSM em `Failover Desativado (pseudo-Standby)`.

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

**Solução**

O problema pode ser a incompatibilidade de atribuição de VLAN no firewall (FWSMs e supervisores). Por exemplo, na instrução Firewall vlan-group 1, o mesmo número de VLANs atribuídas em cada switch ao firewall pode variar. Isso pode causar o problema. Se você atribuir o mesmo número de VLANs no firewall, o failover funcionará.

Para evitar a obtenção de um erro de incompatibilidade de configuração de VLAN, a saída do comando **show vlan** deve ser idêntica em ambos os FWSMs. Esta mensagem de erro ocorre somente quando você modifica ou carrega a configuração de failover no FWSM. Por exemplo, quando um FWSM é inicializado, ele carrega a configuração de inicialização da memória flash e tenta inicializar o failover. Neste momento, ele verifica se ambos os módulos estão recebendo as VLANs corretas. Se as VLANs não corresponderem, a mensagem de erro será exibida e o failover permanecerá desativado.

**Observação:** para que o failover funcione, o FWSM requer configurações e atribuições de porta idênticas. É possível fazer failover entre chassis, mas cada VLAN atribuída ao firewall deve estar no tronco entre os dois chassis.

O FWSM não inclui nenhuma interface física externa. Em vez disso, ele usa interfaces VLAN. Atribuir VLANs ao FWSM é semelhante a atribuir uma VLAN a uma porta de switch. O FWSM inclui uma interface interna para o módulo de matriz de comutação (se houver) ou o barramento compartilhado. Para obter mais informações, consulte Atribuindo VLANs ao Firewall Services Module.

Esteja ciente de que o mapeamento de VLAN pode ser modificado durante uma configuração de FWSM em funcionamento e falhará durante a próxima inicialização.

### Failover Desabilitado

Quando você desabilita o failover usando o comando **no failover**, o estado atual da unidade é mantido (seja ativa ou em espera) até que a unidade seja recarregada. Isso é usado apenas para desativar o failover. Para alterar o estado da unidade de ativo para standby ou vice-versa, você precisa usar o comando **[no] failover ative**.

## Informações Relacionadas

- FWSM: Configurando Failover
- FWSM: Mensagens de log do sistema
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.