

Troubleshooting do Failover FWSM

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Lista de verificação do Failover](#)

[Verifique as relações](#)

[Licenças](#)

[Modo do contexto](#)

[Requisitos de software](#)

[Configuração mínima FWSM para a comutação classificada](#)

[Configuração de switch mínima](#)

[Troubleshooting](#)

[Má combinação da versão](#)

[Licenças incompatíveis](#)

[Modos diferentes \(escolha contra o contexto múltiplo\)](#)

[Dois FWSM tornam-se ativos](#)

[Incompatibilidade de VLAN](#)

[O Failover é desabilitado](#)

[Informações Relacionadas](#)

[Introdução](#)

Este original explica os procedimentos que você pode se usar a fim resolver problemas com a configuração do Failover do módulo firewall service (FWSM).

Este original igualmente fornece uma lista de verificação de procedimentos comuns para tentar antes que você comece a pesquisar defeitos a conexão de failover.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

A informação neste documento é baseada em FWSM 2.3 e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

[Informações de Apoio](#)

A característica do Failover permite que um FWSM à espera tome sobre a funcionalidade de um FWSM falhado. Os dois FWSM envolvidos devem ter a mesma (versão de software principal (primeiro número) e menor, a licença, e os modos operacionais do segundo número) (distribuídos ou transparentes, únicos ou contexto múltiplo). Quando a unidade ativa falhar, as mudanças de estado ao apoio, quando a unidade em standby se mover no estado ativo. Depois que um Failover ocorre, a mesma informação da conexão está disponível na unidade ativa nova.

Para a informação adicional, refira a seção [configurando do Failover de](#) usar o Failover.

[Lista de verificação do Failover](#)

Esta lista de verificação ajuda-o a configurar com sucesso o Failover no FWSM:

- [Verifique as relações](#)
- [Licenças](#)
- [Modo do contexto](#)
- [Requisitos de software](#)
- [Configuração mínima FWSM para a comutação classificada](#)
- [Configuração de switch mínima](#)

[Verifique as relações](#)

Verifique que todas as relações no FWSM têm um endereço IP em standby configurado. Se você não tem feito tão já, configurar o active e os endereços IP em standby para cada relação (modo roteado), ou para o endereço de gerenciamento (modo transparente). O endereço IP em standby é usado no FWSM que é atualmente a unidade em standby. Deve estar na mesma sub-rede como o IP address ativo.

Este é um exemplo de configuração:

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

Nota: Não configurar um IP address para o link failover ou para a relação do estado (se você está indo usar a comutação classificada).

Nota: Você não precisa de identificar a máscara de sub-rede do endereço em standby. O IP address e o MAC address do link failover não mudam no Failover. O IP address ativo para o link failover fica sempre com a unidade primária, quando o endereço IP em standby ficar com a unidade secundária.

Licenças

Ambas as unidades ativa e em standby devem ter a mesma licença.

Modo do contexto

Se a unidade primária reage do único modo do contexto, a unidade secundária deve igualmente reagir no único modo do contexto e do mesmo modo de firewall que a unidade primária.

Se a unidade primária reage do modo de contexto múltiplo, a unidade secundária deve igualmente reagir do modo de contexto múltiplo. Você não precisa de configurar o modo de firewall dos contextos de segurança na unidade secundária porque as relações do Failover e do estado residem no contexto do sistema. A unidade secundária obtém a configuração do contexto de segurança da unidade primária.

Nota: O comando de modo não obtém replicated à unidade secundária.

Nota: O Multicast não é apoiado no modo de contexto múltiplo da ferramenta de segurança. Refira a seção dos [recursos não suportados](#) para mais informação.

Requisitos de software

As duas unidades em uma configuração do Failover devem ter a mesma (versão de software principal (primeiro número) e menor do segundo número). Contudo, você pode usar versões diferentes do software durante um processo de upgrade. Por exemplo, você pode promover uma unidade da versão 3.1(1) à versão 3.1(2) e mandar o Failover permanecer ativo. Cisco recomenda promover ambas as unidades à mesma versão para assegurar a compatibilidade a longo prazo.

Configuração mínima FWSM para a comutação classificada

FWSM preliminar

```
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 de como configurar o Failover ativo e à espera, refira [Failover ativo/à espera configurar](#).

Configuração de switch mínima

- Os VLAN enviados ao FWSM preliminar pelo catalizador que contém o fósforo preliminar da obrigação os VLAN enviamos ao FWSM secundário pelo catalizador que contém o secundário. (Saída da **corrida da mostra | eu** comando do **Firewall** devo ser idêntico.)

Chassi preliminar

```
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
```

- Todos os VLAN que são enviados devem estar presente na base de dados de VLAN e sejam ativos. A fim executar isto, emita estes comandos no interruptor no modo de configuração:

```
vlan 10
no shut
```

A fim verificar se os VLAN estão no base de dados e ativo, a saída do comando **show vlan** em ambos os chassis deve conter os VLAN enviados ao FWSM e mostrá-los como o active. Esta é uma saída de exemplo:

```
Chassi preliminar
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 FWSM têm a Conectividade Layer2 em cada VLAN (devem estar na mesma sub-rede). **Exigências transparentes do Firewall:** A fim evitar laços quando você usa o Failover no modo transparente, você deve usar o software de switch que apoia a transmissão da unidade de dados de protocolo de bridge (PDU). Também, você deve configurar o FWSM para permitir BPDU. A fim permitir BPDU com o FWSM, configurar Ethertype? O ACL e aplica-o a ambas as relações. **Nota:** Ao contrário da plataforma PIX e ASA, o hardware de duas lâminas FWSM é sempre o mesmo, não há nenhuma modelo ou configuração de memória diferente.

Troubleshooting

Quando os reloads FWSM, as encenações explicadas nesta seção farão com que o Failover seja desabilitado.

O FWSM pode recarregar para razões tais como o impacto, restaurou do chassi, reload emitido de FWSM CLI, ou pode apenas ser um módulo novo que seja introduzido ou assentado em um entalhe diferente ou em um apoio posto do chassi.

Má combinação da versão

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

Mensagem do syslog relacionado: [105040](#)

Licenças incompatíveis

Você pôde receber este Syslog devido a uma licença incompatível:

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

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

Mensagens do syslog relacionados: [105045](#) e [105001](#)

Modos diferentes (escolha contra o contexto múltiplo)

o FWSM preliminar e secundário deve reagir do mesmo modo (único ou múltiplo). Por exemplo, se o preliminar está configurado como o modo simples e o secundário enquanto o modo múltiplo e o secundário estão recarregados, a seguir ambos os módulos desligarão o Failover.

Preliminar no modo simples:

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

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

Secundário no modo múltiplo (esta lâmina é recarregada):

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

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

Preliminar no modo múltiplo:

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

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

Mensagens do syslog relacionados: [105044](#), [103001](#), [105001](#)

Dois FWSM tornam-se ativos

Quando você vir este Mensagem de Erro no log:

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

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

A razão para este erro é porque o número recomendado de Canais de porta no interruptor excedeu o máximo (o 128 é máximo no software release 12.2(33)SXH4 do Cisco IOS em Cat6000/6500). Consequentemente, o limite do Interface Descriptor Block (IDB) está sendo esgotado.

Devido a isto, você pôde terminar acima com estas duas edições:

- Quando você tem dois Switches com módulos FWSM cada um a atuar como ativo e à espera, dois módulos FWSM tornam-se ativos ao mesmo tempo.
- Você não pode criar um Canal de porta adicional.

Como parte de resolver a edição, suprima dos Canais de porta que não são precisados e recarregue os FWSM.

Incompatibilidade de VLAN

Problema

O FWSM recebe este Mensagem de Erro: **“Detectou de “Failover do mau combinação da configuração Vlan” de um companheiro ativo” “será desabilitado”**.

OU

A configuração dos módulos firewall service e a configuração de switch correspondente parecem estar completas. Contudo, os FWSM são incapazes à sincronização. Esta mensagem é recebida no host secundário:

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

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

OU

A saída do **comando show failover** mostra que o status de comutação no módulo secundário está, estado do Failover FWSM no `Failover fora (pseudo--à espera)`.

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

Solução

O problema pôde ser a atribuição de VLAN da má combinação através do Firewall (FWSM e supervisores). Por exemplo, na indicação do grupo vlan 1 do Firewall, o mesmo número de VLAN atribuídos em cada interruptor ao Firewall pode variar. Isto pôde causar a edição. Se você atribui o mesmo número de VLAN no Firewall, a seguir o Failover trabalhará.

A fim evitar obter um erro da má combinação da configuração de VLAN, a saída do **comando show vlan** deve ser idêntica em ambos os FWSM. Este Mensagem de Erro ocorre somente quando você altera ou carrega a configuração do Failover no FWSM. Por exemplo, quando um FWSM carreg carrega a partida-configuração do flash e tenta inicializar o Failover. Neste tempo, verifica para certificar-se que ambos os módulos estão recebendo os VLAN corretos. Se os VLAN não combinam, o Mensagem de Erro estão indicados e as sobras do Failover desabilitadas.

Nota: Para que o Failover trabalhe, o FWSM exige configurações idênticas e atribuições de porta. É possível fazer o Failover dos inter-chassis, mas cada VLAN atribuído ao Firewall deve estar no tronco entre os dois chassis.

O FWSM não inclui nenhuma interfaces física externo. Em lugar de, usa interfaces de VLAN. Atribuir VLAN ao FWSM é similar a atribuir um VLAN a uma porta de switch. O FWSM inclui uma interface interna ao módulo switch fabric (se presente) ou ao barramento compartilhado. Para mais informação, refira a [atribuição de VLAN ao módulo de serviços de firewall](#).

Esteja ciente que o mapeamento VLAN pode obter alterado durante uma instalação de trabalho FWSM e falhará durante a bota seguinte.

[O Failover é desabilitado](#)

Quando você desabilita o Failover usando o [comando no failover](#), o estado atual da unidade está mantido (se ativo ou à espera) até a unidade obtém recarregado. Isto é usado para desabilitar somente o Failover. A fim mudar o estado da unidade de ativo ao apoio ou vice versa, você precisa de usar o [comando failover ativo do \[no\]](#).

[Informações Relacionadas](#)

- [FWSM: Configurando o Failover](#)
- [FWSM: Mensagens de Log de sistema](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)