Troubleshooting del Failover FWSM

Contenido

Introducción

Este documento explica los procedimientos que puede utilizar para resolver problemas con la configuración de failover del Módulo de servicio de firewall (FWSM).

Este documento también proporciona una lista de verificación de los procedimientos comunes que debe probar antes de comenzar a resolver problemas de conexión de failover.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en FWSM 2.3 y versiones posteriores.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

La función de failover permite que un FWSM en espera asuma la funcionalidad de un FWSM fallido. Los dos FWSM involucrados deben tener la misma versión de software principal (primer número) y secundaria (segundo número), licencia y modos operativos (enrutados o transparentes, contexto único o múltiple). Cuando la unidad activa falla, el estado cambia a standby, mientras que la unidad standby pasa al estado activo. Después de que ocurre un failover, la misma información de conexión está disponible en la nueva unidad activa.

Para obtener información adicional, consulte la sección Configuración de Failover de Uso de Failover.

Lista de comprobación de fallas

Esta lista de comprobación le ayuda a configurar correctamente la conmutación por fallo en FWSM:

- Verificar las interfaces
- Licencias
- Modo de contexto
- Requisitos de software
- Configuración mínima de FWSM para conmutación por fallo stateful
- Configuración mínima del switch

Verificar las interfaces

Verifique que todas las interfaces en el FWSM tengan una dirección IP standby configurada. Si aún no lo ha hecho, configure las direcciones IP activas y en espera para cada interfaz (modo ruteado) o para la dirección de administración (modo transparente). La dirección IP standby se utiliza en el FWSM que actualmente es la unidad standby. Debe estar en la misma subred que la dirección IP activa.

Este es un ejemplo de configuración:

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

Nota: No configure una dirección IP para el link de failover o para el link de estado (si va a utilizar Stateful Failover).

Nota: No necesita identificar la máscara de subred de la dirección en espera. La dirección IP y la dirección MAC del link de failover no cambian en el failover. La dirección IP activa para el link de failover permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece con la unidad secundaria.

Licencias

Las unidades activas y en espera deben tener la misma licencia.

Modo de contexto

Si la unidad primaria está en modo de contexto único, la unidad secundaria también debe estar en modo de contexto único y en el mismo modo de firewall que la unidad primaria.

Si la unidad primaria está en modo de contexto múltiple, la unidad secundaria también debe estar en modo de contexto múltiple. No necesita configurar el modo de firewall de los contextos de seguridad en la unidad secundaria porque los links de failover y estado residen en el contexto del sistema. La unidad secundaria obtiene la configuración del contexto de seguridad de la unidad primaria.

Nota: El comando **mode** no se replica en la unidad secundaria.

Nota: La multidifusión no se admite en el modo de contexto múltiple del dispositivo de seguridad. Consulte la sección Características no admitidas para obtener más información.

Requisitos de software

Las dos unidades en una configuración de failover deben tener la misma versión de software principal (primer número) y secundaria (segundo número). Sin embargo, puede utilizar diferentes versiones del software durante un proceso de actualización. por ejemplo, usted puede actualizar una unidad de la Versión 3.1(1) a la Versión 3.1(2) y hacer que el failover siga siendo activo. Cisco recomienda actualizar ambas unidades a la misma versión para garantizar la compatibilidad a largo plazo.

Configuración mínima de FWSM para conmutación por fallo stateful

FWSM principal

```
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 secundario

```
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 obtener más información sobre cómo configurar la conmutación por fallas activa y en espera, consulte Configuración de la conmutación por fallas activa/en espera.

Configuración mínima del switch

- Las VLAN enviadas al FWSM principal por el Catalyst que contiene el FWSM principal deben coincidir con las VLAN enviadas al FWSM secundario por el Catalyst que contiene el FWSM secundario. (Salida de **show run | i firewall** debe ser idéntico.)**Chasis 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
```

Chasis secundario

```
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 las VLAN que se envían deben estar presentes en la base de datos de VLAN y deben estar activas.Para realizar esto, ejecute estos comandos en el switch en el modo de configuración:

```
vlan 10
no shut
```

Para verificar si las VLAN están en la base de datos y activas, la salida del comando **show vlan** en ambos chasis debe contener las VLAN enviadas al FWSM y mostrar como activas.Éste es un ejemplo de salida:**Chasis principal**

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

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

Chasis secundario

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

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

- Asegúrese de que los dos FWSM tengan conectividad de capa 2 en cada VLAN (deben estar en la misma subred).**Requisitos de firewall transparente:**Para evitar loops cuando utiliza failover en modo transparente, debe utilizar el software del switch que soporta el reenvío de Bridge Protocol Data Unit (BPDU). Además, debe configurar el FWSM para permitir las BPDU. Para permitir las BPDU a través del FWSM, configure un EtherType? ACL y aplicarla a ambas interfaces.**Nota:** A diferencia de la plataforma PIX y ASA, el hardware de dos blades FWSM es siempre el mismo, no hay modelos ni configuraciones de memoria diferentes.

Resolución de problemas

Cuando se recargue el FWSM, los escenarios explicados en esta sección harán que se inhabilite la conmutación por fallas.

El FWSM puede volver a cargarse por motivos tales como caída, reinicio desde el chasis, recarga emitida desde la CLI del FWSM o simplemente puede ser un nuevo módulo que se inserta o se

vuelve a colocar en una ranura diferente o se alimenta desde el chasis.

Discordancia de versión

Las dos unidades en una configuración de failover deben tener la misma versión de software principal (primer número) y secundaria (segundo número).

Mensaje syslog relacionado: 105040

Licencias incompatibles

Es posible que reciba este registro del sistema debido a una licencia incompatible:

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

Mensajes de syslog relacionados: 105045 y 105001

Diferentes modos (contexto único frente a contexto múltiple)

Tanto el FWSM principal como el secundario deben estar en el mismo modo (único o múltiple). Por ejemplo, si el primario se configura como modo único y el secundario como modo múltiple y el secundario se recarga, entonces ambos módulos desactivarán la conmutación por fallas.

Primario en modo único:

```
%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.
```

Secundario en modo múltiple (este blade se recarga):

```
%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.
```

Primario en modo múltiple:

```
%FWSM-1-105044: (Primary) Mate operational mode (Single) is not compatible
```

```
with my mode (Multi).
%FWSM-1-105001: (Primary) Disabling failover.
```

Mensajes de syslog relacionados: 105044, 103001, 105001

Se activan dos FWSM

Cuando vea este mensaje de error en el registro:

```
fw_create_pc_sw: fw_create_portchannel failed
```

La razón de este error es que el número recomendado de canales de puerto en el switch excedió el máximo (128 es el máximo en la versión 12.2(33)SXH4 del software del IOS de Cisco en Cat6000/6500). Por lo tanto, se está agotando el límite del bloque descriptor de interfaz (IDB).

Debido a esto, es posible que termine con estos dos problemas:

- Cuando tiene dos switches con módulos FWSM que actúan como activos y en espera, dos módulos FWSM se activan al mismo tiempo.
- No puede crear un canal de puerto adicional.

Como parte de la resolución del problema, elimine los canales de puerto que no son necesarios y recargue los FWSM.

Discordancia de VLAN

Problema

El FWSM recibe este mensaje de error: **'Detectado un compañero activo' 'Discordancia de configuración de VLAN' 'Se deshabilitará la conmutación por error'**.

O

La configuración de los módulos de servicio de firewall y la configuración del switch correspondiente parecen estar completas. Sin embargo, los FWSM no pueden sincronizarse entre sí. Este mensaje se recibe en el host secundario:

```
State check detected an Active mate

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

        No Response from Mate
```

O

La salida del comando **show failover** muestra que el estado de failover en el módulo secundario es `OFF`, el estado de failover FWSM en `Failover Off (pseudo-Standby)`.

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

Solución

El problema podría ser la asignación de VLAN no coincidente a través del firewall (FWSM y supervisores). Por ejemplo, en la sentencia Firewall vlan-group 1, el mismo número de VLAN asignadas en cada switch al firewall puede variar. Esto podría causar el problema. Si asigna el mismo número de VLAN en el firewall, la conmutación por fallas funcionará.

Para evitar un error de discordancia de configuración de VLAN, el resultado del comando **show vlan** debe ser idéntico en ambos FWSM. Este mensaje de error sólo se produce cuando modifica o carga la configuración de conmutación por error en el FWSM. Por ejemplo, cuando un FWSM arranca, carga la configuración de inicio desde la memoria flash e intenta inicializar la conmutación por error. En este momento, verifica que ambos módulos estén recibiendo las VLAN correctas. Si las VLAN no coinciden, se muestra el mensaje de error y la conmutación por fallas permanece inhabilitada.

Nota: Para que la conmutación por fallo funcione, el FWSM requiere configuraciones y asignaciones de puertos idénticos. Es posible realizar una conmutación por fallas entre chasis, pero cada VLAN asignada al firewall debe estar en el trunk entre los dos chasis.

FWSM no incluye ninguna interfaz física externa. En su lugar, utiliza las interfaces de las VLAN. La asignación de VLAN al FWSM es similar a la asignación de una VLAN a un puerto de switch. El FWSM incluye una interfaz interna con el módulo de fabric de switch (si existe) o el bus compartido. Para obtener más información, consulte Asignación de VLAN al Módulo de Servicios de Firewall.

Tenga en cuenta que la asignación de VLAN se puede modificar durante una configuración FWSM en funcionamiento y fallará durante el siguiente arranque.

La conmutación por fallas está inhabilitada

Cuando inhabilita el failover usando el comando no failover , el estado actual de la unidad se mantiene (si está activa o en espera) hasta que la unidad se recarga. Esto se utiliza solamente para inhabilitar el failover. Para cambiar el estado de la unidad de activa a standby o viceversa, debe utilizar el comando [no] failover active.

Información Relacionada

- FWSM: Configuración de Failover
- FWSM: Mensajes del registro del sistema
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).