FWSM-failover voor probleemoplossing

Inhoud

Inleiding

Dit document legt de procedures uit die u kunt gebruiken om problemen met de FWSM-configuratie (Firewall Service Module) op te lossen.

Dit document bevat ook een controlelijst van de gebruikelijke procedures die u moet proberen voordat u de failover-verbinding kunt oplossen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op FWSM 2.3 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

De failover-functie stelt een stand-by FWSM in staat om de functionaliteit van een mislukte FWSM over te nemen. De twee betrokken FWSM's moeten dezelfde hoofdversie (eerste nummer) en kleinere softwareversie (tweede nummer), licentie en besturingsmodi hebben (gerouteerd of transparant, enkele of meerdere context). Als de actieve unit uitvalt, verandert de status in stand-by, terwijl de stand-by unit naar de actieve status verplaatst. Nadat een failover is opgetreden, is dezelfde verbindingsinformatie beschikbaar op de nieuwe actieve unit.

Raadpleeg de sectie failover configureren van het gebruik van failover voor aanvullende informatie.

failover-checklist

Deze controlelijst helpt u de failover in FWSM met succes te configureren:

- Controleer de interfaces
- Licenties
- Contextmodus
- Softwarevereisten
- Minimale FWSM-configuratie voor stateful failover
- Minimale Switch-configuratie

Controleer de interfaces

Controleer of alle interfaces op de FWSM een geconfigureerd stand-by IP-adres hebben. Als u dit nog niet hebt gedaan, configureer dan de actieve en stand-by IP-adressen voor elke interface (routed mode) of voor het beheeradres (transparante modus). Het standby IP-adres wordt gebruikt op de FWSM die momenteel de standby-unit is. Het moet in hetzelfde subnetje staan als het actieve IP-adres.

Hierna volgt een configuratievoorbeeld:

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

Opmerking: configureer geen IP-adres voor de failover-link of voor de stateful link (als u Stateful failover gaat gebruiken).

Opmerking: U hoeft het standby-adressubnetmasker niet te identificeren. Het IP-adres van de failover-link en het MAC-adres veranderen niet bij failover. Het actieve IP-adres voor de failover-link blijft altijd bij de primaire eenheid, terwijl het standby IP-adres bij de secundaire eenheid blijft.

Licenties

Zowel actieve als stand-by eenheden moeten over dezelfde licentie beschikken.

Contextmodus

Als de primaire eenheid zich in één contextmodus bevindt, moet de secundaire eenheid zich ook in één contextmodus bevinden en in dezelfde firewallmodus als de primaire eenheid.

Als de primaire eenheid zich in een meervoudige contextmodus bevindt, moet de secundaire eenheid zich ook in een meervoudige contextmodus bevinden. U hoeft de firewallmodus van de beveiligingscontexten op de secundaire eenheid niet te configureren omdat de failover- en state-koppelingen zich in de systeemcontext bevinden. De secundaire eenheid verkrijgt de configuratie van de veiligheidscontext uit de primaire eenheid.

Opmerking: de opdracht **modus** wordt niet gerepliceerd naar de secundaire eenheid.

N.B.: Multicast wordt niet ondersteund in de multiple context modus van het security apparaat. Raadpleeg het gedeelte Niet-ondersteunde functies voor meer informatie.

Softwarevereisten

De twee eenheden in een failoverconfiguratie moeten dezelfde grote (eerste nummer) en kleinere (tweede nummer) softwareversie hebben. U kunt echter tijdens een upgrade verschillende versies van de software gebruiken. U kunt bijvoorbeeld één eenheid upgraden van Versie 3.1(1) naar Versie 3.1(2) en failover actief laten blijven. Cisco raadt aan beide eenheden te upgraden naar dezelfde versie om de compatibiliteit op lange termijn te garanderen.

Minimale FWSM-configuratie voor stateful failover

Primair 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
```

Secundair 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
```

Raadpleeg Active/stand-by failover configureren voor meer informatie over het configureren van Active/stand-by failover.

Minimale Switch-configuratie

- VLAN's die door de Catalyst naar het primaire FWSM worden verzonden en het primaire FWSM bevatten, moeten overeenkomen met de VLAN's die door de Catalyst met het secundaire FWSM worden verzonden. (Uitvoer van de **show | i de** opdracht **firewall** moet identiek zijn.)**Primair chassis**

```
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
```

Secundair chassis

```
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
```

- Alle VLAN's die worden verzonden, moeten aanwezig zijn in de VLAN-database en actief zijn.Om dit uit te voeren, geef deze opdrachten in de switch in configuratiemodus uit:

```
vlan 10
no shut
```

Om te verifiëren als VLANs in het gegevensbestand en actief zijn, moet de output van het **show VLAN** bevel op beide chassis VLANs bevatten die naar FWSM worden verzonden en actief tonen.Dit is een voorbeelduitvoer:**Primair chassis**

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

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

Secundair chassis

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

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

- Zorg ervoor dat de twee FWSM's Layer 2-connectiviteit in elk VLAN hebben (ze moeten in hetzelfde subnetje staan).**Transparante firewallvereisten:**Om lusjes te vermijden wanneer u failover op transparante wijze gebruikt, moet u switch software gebruiken die het door:sturen van de Eenheid van de Gegevens van het Protocol van de Brug (BPDU) steunt. Ook, moet u FWSM vormen om BPDUs toe te staan. Om BPDUs door FWSM toe te staan, een EtherType vormen? ACL toe te passen op beide interfaces.**Opmerking:** in tegenstelling tot het PIX- en ASA-platform is de hardware van twee FWSM-blades altijd hetzelfde, er zijn geen verschillende modellen of geheugenconfiguraties.

Probleemoplossing

Wanneer de FWSM opnieuw wordt geladen, zullen de scenario's die in deze sectie worden beschreven ervoor zorgen dat failover wordt uitgeschakeld.

De FWSM kan herladen om redenen zoals crash, gereset vanuit het chassis, herladen uitgegeven vanuit FWSM CLI, of het kan gewoon een nieuwe module zijn die is geplaatst of opnieuw gecreëerd in een andere sleuf of aangedreven back-up van het chassis.

Versie Mismatch

De twee eenheden in een failoverconfiguratie moeten dezelfde grote (eerste nummer) en kleinere (tweede nummer) softwareversie hebben.

Verwante syslog melding: 105040

Incompatibele licenties

Mogelijk ontvangt u deze syslog vanwege een niet-compatibele licentie:

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

Verwante syslog berichten: 105045 en 105001

Verschillende modi (enkelvoudige versus meervoudige context)

Zowel het primaire als het secundaire FWSM moet in dezelfde modus (enkelvoudig of meervoudig) staan. Als de primaire modus bijvoorbeeld is ingesteld op één modus en de secundaire modus op meerdere modi en de secundaire modus opnieuw wordt geladen, zullen beide modules failover uitschakelen.

Primair in enkelvoudige modus:

```
%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.
```

Secundair in meervoudige modus (dit blad wordt opnieuw geladen):

```
%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.
```

Primair in multi-mode:

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

Verwante syslog berichten: 105044, 103001, 105001

Twee FWSM's worden actief

Wanneer u deze foutmelding in het logbestand ziet:

```
fw_create_pc_sw: fw_create_portchannel failed
```

De reden voor deze fout is dat het aanbevolen aantal poortkanalen in de switch het maximum (128 is maximum in Cisco IOS-softwarerelease 12.2(33)SXH4 op Cat6000/6500) heeft overschreden. Daarom wordt de limiet van Interface Descriptor Block (IDB) opgebruikt.

Hierdoor kom je misschien terecht bij deze twee kwesties:

- Wanneer u twee switches met FWSM modules elk hebt om als actief en stand-by te handelen, worden twee FWSM modules tegelijkertijd actief.
- U kunt geen extra poortkanaal maken.

Als onderdeel van het oplossen van het probleem, verwijder de poortkanalen die niet nodig zijn en herlaad de FWSM's.

VLAN-fout

Probleem

FWSM ontvangt deze foutmelding: **'Gedetecteerd een Active Mate' 'VLAN-configuratiefout' 'failover wordt uitgeschakeld'**.

OF

De configuratie van de firewallservicemodules en de bijbehorende switch-configuratie lijken volledig te zijn. De FWSM's kunnen elkaar echter niet synchroniseren. Dit bericht wordt ontvangen op de secundaire host:

```
State check detected an Active mate

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

        No Response from Mate
```

OF

De output van de opdracht **show failover** toont dat de failoverstatus op de secundaire module `OFF` is, FWSM failover status in `failover Off (pseudo-Standby)`.

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

Oplossing

Het probleem kan de foute VLAN-toewijzing over de firewall (FWSM's en supervisors) zijn. In de

verklaring Firewall VLAN-group 1 kan bijvoorbeeld hetzelfde aantal VLAN's dat op elke switch aan de firewall is toegewezen, variëren. Dit zou de kwestie kunnen veroorzaken. Als u hetzelfde aantal VLAN's in de firewall toewijst, werkt failover.

Om te vermijden verkrijgend een fout van de de configuratiewanverhouding van VLAN, moet de **show VLAN** beveloutput op beide FWSMs identiek zijn. Deze foutmelding wordt alleen weergegeven wanneer u de failover-configuratie op FWSM aanpast of laadt. Bijvoorbeeld, wanneer een FWSM start laadt het het opstarten -opstarten -configureren van de flitser en probeert failover te initialiseren. Op dit moment controleert het of beide modules de juiste VLAN's ontvangen. Als de VLAN's niet overeenkomen, wordt de foutmelding weergegeven en blijft failover uitgeschakeld.

Opmerking: voor failover om te werken, vereist de FWSM identieke configuraties en poorttoewijzingen. Het is mogelijk om interchassis failover te doen, maar elk VLAN dat aan de firewall is toegewezen moet zich in de trunk tussen de twee chassis bevinden.

FWSM omvat geen externe fysieke interfaces. In plaats daarvan maakt het gebruik van VLAN-interfaces. De toewijzing van VLAN's aan FWSM is vergelijkbaar met de toewijzing van een VLAN aan een switch poort. FWSM bevat een interfaceinterface met de Switch Fabric Module (indien aanwezig) of de gedeelde bus. Raadpleeg voor meer informatie VLAN's toewijzen aan de firewallservicesmodule.

Houd er rekening mee dat de VLAN-toewijzing kan worden gewijzigd tijdens een werkende FWSM-installatie en zal mislukken tijdens de volgende opstart.

failover is uitgeschakeld

Wanneer u de failover uitschakelt met de opdracht geen failover, blijft de huidige status van de eenheid behouden (actief of stand-by) totdat de eenheid opnieuw wordt geladen. Dit wordt alleen gebruikt om de failover uit te schakelen. Om de status van de unit te wijzigen van active naar standby of vice versa, moet u de [no] failover active-opdracht gebruiken.

Gerelateerde informatie

- FWSM: failover configureren
- FWSM: Systeemlogberichten
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.