Risoluzione dei problemi di failover FWSM

Sommario

Introduzione

Questo documento spiega le procedure da utilizzare per risolvere i problemi relativi alla configurazione del failover del Firewall Service Module (FWSM).

In questo documento viene inoltre fornito un elenco di controllo delle procedure comuni da eseguire prima di iniziare a risolvere i problemi relativi alla connessione di failover.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 2.3 di FWSM e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

La funzione di failover consente a un modulo FWSM in standby di acquisire la funzionalità di un modulo FWSM guasto. I due FWSM interessati devono avere la stessa versione del software, la stessa licenza e le stesse modalità operative principali (primo numero) e secondarie (secondo numero) (instradate o trasparenti, a contesto singolo o multiplo). Quando l'unità attiva non funziona, lo stato passa allo stato di standby, mentre l'unità di standby passa allo stato attivo. Dopo un failover, le stesse informazioni di connessione sono disponibili nella nuova unità attiva.

Per ulteriori informazioni, vedere la sezione Configurazione del failover in Utilizzo del failover.

Elenco di controllo per il failover

Questo elenco di controllo consente di configurare correttamente il failover in FWSM:

- Verifica delle interfacce
- Licenze
- Modalità contesto
- Requisiti software
- Configurazione minima FWSM per failover stateful
- Configurazione minima dello switch

Verifica delle interfacce

Verificare che tutte le interfacce nel modulo FWSM dispongano di un indirizzo IP di standby configurato. Se non è già stato fatto, configurare gli indirizzi IP attivo e in standby per ciascuna interfaccia (modalità instradata) o per l'indirizzo di gestione (modalità trasparente). L'indirizzo IP di standby viene utilizzato sull'FWSM che attualmente è l'unità di standby. Deve trovarsi nella stessa subnet dell'indirizzo IP attivo.

Di seguito viene riportata una configurazione di esempio:

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

Nota: non configurare un indirizzo IP per il collegamento di failover o per il collegamento di stato (se si intende utilizzare il failover stateful).

Nota: non è necessario identificare la subnet mask dell'indirizzo di standby. L'indirizzo IP e l'indirizzo MAC del collegamento di failover non cambiano al momento del failover. L'indirizzo IP attivo per il collegamento di failover rimane sempre associato all'unità principale, mentre l'indirizzo IP di standby rimane associato all'unità secondaria.

Licenze

Le unità attive e quelle in standby devono avere la stessa licenza.

Modalità contesto

Se l'unità primaria è in modalità contesto singolo, anche l'unità secondaria deve essere in modalità contesto singolo e nella stessa modalità firewall dell'unità primaria.

Se l'unità primaria è in modalità contesto multiplo, anche l'unità secondaria deve essere in modalità contesto multiplo. Non è necessario configurare la modalità firewall dei contesti di sicurezza sull'unità secondaria, in quanto i collegamenti di stato e di failover risiedono nel contesto di sistema. L'unità secondaria ottiene la configurazione del contesto di sicurezza dall'unità primaria.

Nota: il comando **mode** non viene replicato nell'unità secondaria.

Nota: il multicast non è supportato nella modalità contesto multiplo dell'accessorio di protezione. Per ulteriori informazioni, consultare la sezione Feature non supportate.

Requisiti software

Le due unità in una configurazione di failover devono avere la stessa versione del software principale (primo numero) e secondaria (secondo numero). Tuttavia, è possibile utilizzare versioni diverse del software durante un processo di aggiornamento. Ad esempio, è possibile aggiornare un'unità dalla versione 3.1(1) alla versione 3.1(2) e mantenere attivo il failover. Cisco consiglia di aggiornare entrambe le unità alla stessa versione per garantire la compatibilità a lungo termine.

Configurazione minima FWSM per failover stateful

FWSM primario

```
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 secondario

```
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
```

Per ulteriori informazioni su come configurare il failover attivo e in standby, vedere Configurazione del failover attivo/in standby.

Configurazione minima dello switch

- Le VLAN inviate all'FWSM primario dal Catalyst che contiene il server primario devono corrispondere alle VLAN inviate all'FWSM secondario dal Catalyst che contiene il server secondario. (Output del comando **show run | i** il comando **firewall** deve essere identico.)**Chassis principale**

```
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
```

Chassis secondario

```
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
```

- Tutte le VLAN inviate devono essere presenti nel database VLAN e attive.Per eseguire questa operazione, usare i seguenti comandi sullo switch in modalità di configurazione:

```
vlan 10
no shut
```

Per verificare se le VLAN sono nel database e attive, l'output del comando **show vlan** su entrambi gli chassis deve contenere le VLAN inviate al modulo FWSM e mostrate come attive.Di seguito viene riportato un esempio di output:**Chassis principale**

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

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

Chassis secondario

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

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

- Verificare che i due FWSM dispongano di connettività di layer 2 in ciascuna VLAN (devono trovarsi nella stessa subnet).**Requisiti per il firewall trasparente:**Per evitare loop quando si utilizza il failover in modalità trasparente, è necessario utilizzare un software di switch che supporti l'inoltro BDPU (Bridge Protocol Data Unit). Inoltre, è necessario configurare il modulo FWSM in modo da consentire le BPDU. Per consentire le BPDU tramite l'FWSM, configurare un EtherType? e applicarlo a entrambe le interfacce.**Nota:** a differenza delle piattaforme PIX e ASA, l'hardware di due blade FWSM è sempre lo stesso, non esistono modelli o configurazioni di memoria diversi.

Risoluzione dei problemi

Quando il modulo FWSM viene ricaricato, gli scenari illustrati in questa sezione provocheranno la disabilitazione del failover.

L'FWSM può essere ricaricato per motivi quali crash, reset dal telaio, ricaricamento emesso dalla

CLI dell'FWSM, o può semplicemente essere un nuovo modulo inserito o riposizionato in un altro slot o riacceso dallo chassis.

Versione non corrispondente

Le due unità in una configurazione di failover devono avere la stessa versione del software principale (primo numero) e secondaria (secondo numero).

Messaggio syslog correlato: 105040

Licenze incompatibili

Il syslog potrebbe essere ricevuto a causa di una licenza non compatibile:

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

Messaggi syslog correlati: 105045 e 105001

Modalità diverse (contesto singolo o multiplo)

Sia l'FWSM primario che quello secondario devono trovarsi nella stessa modalità (uno o più). Ad esempio, se la modalità primaria è configurata come modalità singola e la modalità secondaria come modalità multipla e la modalità secondaria viene ricaricata, entrambi i moduli disattiveranno il failover.

Principale in modalità singola:

```
%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.
```

Secondario in modalità multipla (questo blade viene ricaricato):

```
%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.
```

Principale in modalità multipla:

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

Messaggi syslog correlati: 105044, 103001, 105001

Due FWSM diventano attivi

Quando viene visualizzato questo messaggio di errore nel registro:

```
fw_create_pc_sw: fw_create_portchannel failed
```

Questo errore si verifica perché il numero di canali della porta consigliato nello switch supera il numero massimo (128 corrisponde al numero massimo nel software Cisco IOS versione 12.2(33)SXH4 su Cat6000/6500). Il limite IDB (Interface Descriptor Block) è stato pertanto esaurito.

Per questo motivo, è possibile che si verifichino i due problemi seguenti:

- Quando si hanno due switch con moduli FWSM ciascuno che agiscono come attivo e in standby, due moduli FWSM diventano attivi contemporaneamente.
- Non è possibile creare un canale porta aggiuntivo.

Per risolvere il problema, eliminare i canali porte non necessari e ricaricare gli FWSM.

VLAN non corrispondente

Problema

Viene visualizzato il seguente messaggio di errore: '**Rilevato un accoppiamento attivo**' '**Configurazione VLAN non corrispondente**' '**il failover verrà disabilitato**'.

O

La configurazione dei moduli del servizio firewall e la configurazione dello switch corrispondente sembrano essere complete. I moduli FWSM non sono tuttavia in grado di sincronizzarsi. Questo messaggio viene ricevuto sull'host secondario:

```
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

L'output del comando **show failover** visualizza lo stato del failover sul modulo secondario: `OFF`, lo stato del failover del modulo FWSM in `Failover Off (pseudo standby)`.

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

Soluzione

Il problema potrebbe essere la mancata corrispondenza dell'assegnazione della VLAN attraverso il firewall (FWSM e supervisori). Ad esempio, nell'istruzione Firewall vlan-group 1, lo stesso numero di VLAN assegnate su ciascuno switch al firewall può variare. Ciò potrebbe causare il problema. Se si assegna lo stesso numero di VLAN nel firewall, il failover funzionerà.

Per evitare di ricevere un errore di configurazione VLAN non corrispondente, l'output del comando **show vlan** deve essere identico su entrambi gli FWSM. Questo messaggio di errore viene visualizzato solo quando si modifica o si carica la configurazione di failover nel modulo FWSM. Ad esempio, quando si avvia un FWSM, carica la configurazione di avvio dalla memoria flash e tenta di inizializzare il failover. In questo momento, controlla che entrambi i moduli ricevano le VLAN corrette. Se le VLAN non corrispondono, viene visualizzato il messaggio di errore e il failover rimane disabilitato.

Nota: affinché il failover funzioni correttamente, FWSM richiede configurazioni e assegnazioni di porte identiche. È possibile eseguire il failover tra chassis, ma ciascuna VLAN assegnata al firewall deve trovarsi nel trunk tra i due chassis.

Il modulo FWSM non include interfacce fisiche esterne. ma utilizza interfacce VLAN. L'assegnazione delle VLAN all'FWSM è simile all'assegnazione di una VLAN a una porta dello switch. L'FWSM include un'interfaccia interna allo switch fabric module (se presente) o al bus condiviso. Per ulteriori informazioni, consultare il documento sull'assegnazione delle VLAN al modulo Firewall Services.

Tenere presente che la mappatura VLAN può essere modificata durante una configurazione FWSM funzionante e non riesce al successivo avvio.

Failover disabilitato

Quando si disabilita il failover con il comando no failover, lo stato corrente dell'unità viene mantenuto (attivo o in standby) fino a quando non viene ricaricata. Questa opzione viene utilizzata solo per disabilitare il failover. Per modificare lo stato dell'unità da attivo a standby o viceversa, è necessario usare il comando [no] failover attivo.

Informazioni correlate

- FWSM: Configurazione del failover
- FWSM: Messaggi registro di sistema
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).