FWSM-Failover-Fehlerbehebung

Inhalt

Einleitung

In diesem Dokument werden die Verfahren erläutert, die Sie zur Behebung von Problemen mit der Failover-Konfiguration des Firewall-Servicemoduls (FWSM) verwenden können.

In diesem Dokument finden Sie außerdem eine Checkliste gängiger Verfahren, die Sie ausprobieren sollten, bevor Sie mit der Fehlerbehebung für die Failover-Verbindung beginnen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf FWSM 2.3 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Mithilfe der Failover-Funktion kann ein Standby-FWSM die Funktionalität eines ausgefallenen FWSM übernehmen. Die beiden beteiligten FWSMs müssen über die gleiche Haupt- (erste Nummer) und Nebenversion, die gleiche Lizenz und den gleichen Betriebsmodus (geroutet oder transparent, mit einem oder mehreren Kontexten) verfügen. Wenn das aktive Gerät ausfällt, wechselt der Status in den Standby-Status, während das Standby-Gerät in den aktiven Status wechselt. Nach einem Failover sind die gleichen Verbindungsinformationen an der neuen aktiven Einheit verfügbar.

Weitere Informationen finden Sie im Abschnitt Failover konfigurieren unter Failover verwenden.

Failover-Checkliste

Mithilfe dieser Checkliste können Sie das Failover in FWSM erfolgreich konfigurieren:

- Überprüfen der Schnittstellen
- Lizenzen
- Kontextmodus
- Software-Mindestanforderungen
- Minimale FWSM-Konfiguration für Stateful Failover
- Minimale Switch-Konfiguration

Überprüfen der Schnittstellen

Überprüfen Sie, ob alle Schnittstellen auf dem FWSM über eine konfigurierte Standby-IP-Adresse verfügen. Falls noch nicht geschehen, konfigurieren Sie die aktiven und Standby-IP-Adressen für jede Schnittstelle (gerouteter Modus) oder die Management-Adresse (transparenter Modus). Die Standby-IP-Adresse wird auf dem FWSM verwendet, das derzeit die Standby-Einheit ist. Sie muss sich im gleichen Subnetz wie die aktive IP-Adresse befinden.

Unten sehen Sie eine Beispielkonfiguration:

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

Hinweis: Konfigurieren Sie keine IP-Adresse für die Failover-Verbindung oder die State-Verbindung (wenn Sie Stateful Failover verwenden).

Hinweis: Sie müssen die Subnetzmaske der Standby-Adresse nicht identifizieren. Die IP-Adresse und die MAC-Adresse der Failover-Verbindung ändern sich beim Failover nicht. Die aktive IP-Adresse für die Failover-Verbindung bleibt immer bei der primären Einheit, während die Standby-IP-Adresse bei der sekundären Einheit bleibt.

Lizenzen

Sowohl aktive als auch Standby-Geräte müssen über dieselbe Lizenz verfügen.

Kontextmodus

Wenn sich die primäre Einheit im Single-Context-Modus befindet, muss sich die sekundäre Einheit ebenfalls im Single-Context-Modus und im gleichen Firewall-Modus wie die primäre Einheit befinden.

Wenn sich die primäre Einheit im Mehrfachkontextmodus befindet, muss sich die sekundäre Einheit ebenfalls im Mehrfachkontextmodus befinden. Sie müssen den Firewall-Modus der Sicherheitskontexte auf der sekundären Einheit nicht konfigurieren, da sich die Failover- und Status-Links im Systemkontext befinden. Die sekundäre Einheit erhält die Konfiguration des Sicherheitskontexts von der primären Einheit.

Hinweis: Der Befehl **mode** wird nicht auf die sekundäre Einheit repliziert.

Hinweis: Multicast wird im Multiple-Context-Modus der Security Appliance nicht unterstützt. Weitere Informationen finden Sie im Abschnitt Nicht unterstützte Funktionen.

Software-Mindestanforderungen

Die beiden Einheiten in einer Failover-Konfiguration müssen die gleiche Haupt- (erste Zahl) und Nebenversion der Software (zweite Zahl) aufweisen. Sie können jedoch während eines Upgrade-Vorgangs verschiedene Versionen der Software verwenden. Sie können beispielsweise ein Upgrade von Version 3.1(1) auf Version 3.1(2) durchführen, während Failover aktiv bleibt. Cisco empfiehlt zur Gewährleistung der langfristigen Kompatibilität ein Upgrade beider Systeme auf dieselbe Version.

Minimale FWSM-Konfiguration für Stateful Failover

Primärer 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
```

Sekundäres 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
```

Weitere Informationen zum Konfigurieren von aktivem und Standby-Failover finden Sie unter

Konfigurieren von aktivem/Standby-Failover.

Minimale Switch-Konfiguration

- Die VLANs, die der Catalyst mit dem primären FWSM sendet, müssen mit den VLANs übereinstimmen, die der Catalyst mit dem sekundären FWSM sendet. (Ausgabe des **Showlaufs | i Firewall**-Befehl muss identisch sein.)**Primäres 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
```

Sekundäres 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 gesendeten VLANs müssen in der VLAN-Datenbank vorhanden und aktiv sein.Führen Sie dazu im Konfigurationsmodus die folgenden Befehle am Switch aus:

```
vlan 10
no shut
```

Um zu überprüfen, ob die VLANs in der Datenbank vorhanden und aktiv sind, muss die Ausgabe des Befehls **show vlan** auf beiden Chassis die an den FWSM gesendeten VLANs enthalten, die als aktiv angezeigt werden.Dies ist eine Beispielausgabe:**Primäres Chassis**

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

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

Sekundäres Chassis

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

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

- Stellen Sie sicher, dass die beiden FWSMs über Layer-2-Verbindungen in jedem VLAN verfügen (sie müssen sich im gleichen Subnetz befinden).**Transparente Firewall-Anforderungen:**Um Schleifen zu vermeiden, wenn Sie Failover im transparenten Modus verwenden, müssen Sie eine Switch-Software verwenden, die die Bridge Protocol Data Unit (BPDU)-Weiterleitung unterstützt. Außerdem müssen Sie FWSM so konfigurieren, dass BPDUs zulässig sind. Konfigurieren Sie einen EtherType, um BPDUs über FWSM zuzulassen? ACLs und wenden sie auf beide Schnittstellen an.**Hinweis:** Im Gegensatz zur PIX- und ASA-Plattform ist die Hardware von zwei FWSM-Blades immer gleich. Es gibt keine unterschiedlichen Modelle oder Speicherkonfigurationen.

Fehlerbehebung

Wenn das FWSM neu geladen wird, werden die in diesem Abschnitt beschriebenen Szenarien

das Failover deaktivieren.

Das FWSM kann aus Gründen wie Absturz, Zurücksetzen vom Chassis, von der FWSM-CLI ausgegebenes Neuladen oder einfach ein neues Modul sein, das in einen anderen Steckplatz eingesetzt oder wieder eingesetzt oder vom Chassis hochgefahren wird.

Versionskonflikt

Die beiden Einheiten in einer Failover-Konfiguration müssen die gleiche Haupt- (erste Zahl) und Nebenversion der Software (zweite Zahl) aufweisen.

Zugehörige Syslog-Meldung: 105040

Inkompatible Lizenzen

Möglicherweise erhalten Sie dieses Syslog aufgrund einer inkompatiblen Lizenz:

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

Zugehörige Syslog-Meldungen: 105045 und 105001

Verschiedene Modi (einzelner oder mehrerer Kontext)

Sowohl das primäre als auch das sekundäre FWSM müssen sich im gleichen Modus befinden (Single oder Multiple). Wenn beispielsweise der primäre Modus als Einzelmodus und der sekundäre Modus als Mehrfachmodus konfiguriert und der sekundäre Modus neu geladen wird, deaktivieren beide Module den Failover.

Primär im Einzelmodus:

```
%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.
```

Sekundär im Mehrfachmodus (dieser Blade wird neu 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.
```

Primär im Mehrfachmodus:

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

Zugehörige Syslog-Meldungen: 10504, 103001, 105001

Zwei FWSMs werden aktiv

Wenn diese Fehlermeldung im Protokoll angezeigt wird:

```
fw_create_pc_sw: fw_create_portchannel failed
```

Der Grund für diesen Fehler liegt darin, dass die empfohlene Anzahl von Port-Channels im Switch den Maximalwert überschritten hat (128 ist der Maximalwert in Version 12.2(33)SXH4 der Cisco IOS-Software für Catalyst 6000/6500). Der IDB-Grenzwert (Interface Descriptor Block) wird daher überschritten.

Aus diesem Grund könnten am Ende folgende zwei Probleme auftreten:

- Wenn zwei Switches mit FWSM-Modulen jeweils als aktive und Standby-Switches fungieren, werden zwei FWSM-Module gleichzeitig aktiv.
- Sie können keinen zusätzlichen Port-Channel erstellen.

Um das Problem zu beheben, löschen Sie die nicht benötigten Port-Channels, und laden Sie die FWSMs neu.

VLAN-Nichtübereinstimmung

Problem

FWSM empfängt die folgende Fehlermeldung: '**Active Mate erkannt**' '**VLAN-Konfigurationskonflikt**' '**Failover wird deaktiviert**'.

ODER

Die Konfiguration der Firewall-Service-Module und der entsprechenden Switch-Konfiguration scheint abgeschlossen zu sein. Die FWSMs können jedoch nicht miteinander synchronisiert werden. Diese Nachricht wird auf dem sekundären Host empfangen:

```
State check detected an Active mate

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

        No Response from Mate
```

ODER

Die Ausgabe des Befehls **show failover** gibt an, dass der Failover-Status auf dem sekundären Modul `OFF` ist, der FWSM-Failover-Status `Failover Off (Pseudo-Standby)`.

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

Lösung

Das Problem kann in der unterschiedlichen VLAN-Zuweisung über die Firewall (FWSMs und Supervisoren) bestehen. In der Anweisung "Firewall vlan-group 1" kann beispielsweise die gleiche Anzahl von VLANs variieren, die der Firewall auf jedem Switch zugewiesen sind. Dies kann das Problem verursachen. Wenn Sie der Firewall dieselbe Anzahl von VLANs zuweisen, funktioniert Failover.

Um einen VLAN-Konfigurationsfehler zu vermeiden, muss der Befehl **show vlan** auf beiden FWSMs identisch sein. Diese Fehlermeldung wird nur angezeigt, wenn Sie die Failover-Konfiguration auf FWSM ändern oder laden. Wenn beispielsweise ein FWSM bootet, lädt es die Startkonfiguration aus dem Flash-Speicher und versucht, das Failover zu initialisieren. Zu diesem Zeitpunkt wird überprüft, ob beide Module die richtigen VLANs empfangen. Wenn die VLANs nicht übereinstimmen, wird die Fehlermeldung angezeigt, und Failover bleibt deaktiviert.

Hinweis: Damit Failover funktioniert, benötigt das FWSM identische Konfigurationen und Portzuweisungen. Es ist möglich, ein Inter-Chassis-Failover durchzuführen, aber jedes der Firewall zugewiesene VLAN muss sich im Trunk zwischen den beiden Chassis befinden.

FWSM enthält keine externen physischen Schnittstellen. Stattdessen werden VLAN-Schnittstellen verwendet. Das Zuweisen von VLANs zum FWSM ähnelt dem Zuweisen eines VLAN zu einem Switch-Port. Das FWSM umfasst eine interne Schnittstelle zum Switch-Fabric-Modul (falls vorhanden) oder zum gemeinsam genutzten Bus. Weitere Informationen finden Sie unter Zuweisen von VLANs zum Firewall Services-Modul.

Beachten Sie, dass die VLAN-Zuordnung während einer FWSM-Einrichtung geändert werden kann und beim nächsten Start fehlschlägt.

Failover ist deaktiviert

Wenn Sie den Failover mit dem Befehl no failover deaktivieren, wird der aktuelle Status des Geräts (aktiv oder Standby) beibehalten, bis das Gerät neu geladen wird. Diese wird nur verwendet, um den Failover zu deaktivieren. Um den Status des Geräts von "Aktiv" in "Standby" oder umgekehrt zu ändern, müssen Sie den Befehl [no] failover active verwenden.

Zugehörige Informationen

- FWSM: Konfigurieren von Failover
- FWSM: Systemprotokollmeldungen
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.