Dépannage du basculement FWSM

Contenu

Introduction

Ce document explique les procédures que vous pouvez utiliser afin de résoudre les problèmes avec la configuration de basculement du module de service de pare-feu (FWSM).

Ce document fournit également une liste de contrôle des procédures courantes à essayer avant de commencer à dépanner la connexion de basculement.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur FWSM 2.3 et versions ultérieures.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

La fonctionnalité de basculement permet à un FWSM de secours de prendre le relais de la fonctionnalité d'un FWSM défaillant. Les deux FWSM concernés doivent avoir la même version logicielle majeure (premier numéro) et mineure (deuxième numéro), la même licence et les mêmes modes de fonctionnement (routé ou transparent, contexte unique ou multiple). Lorsque l'unité active tombe en panne, l'état passe à l'état de veille, tandis que l'unité en veille passe à l'état actif. Lorsqu'un basculement s'est produit, les mêmes informations de connexion sont disponibles sur la nouvelle unité active.

Pour plus d'informations, référez-vous à la section Configuration du basculement de Utilisation du basculement.

Liste de contrôle de basculement

Cette liste de contrôle vous aide à configurer correctement le basculement dans FWSM :

- Vérification des interfaces
- Licences
- Mode contextuel
- Configuration logicielle requise
- Configuration FWSM minimale pour le basculement dynamique
- Configuration minimale du commutateur

Vérification des interfaces

Vérifiez que toutes les interfaces du FWSM ont une adresse IP de secours configurée. Si ce n’est déjà fait, configurez les adresses IP active et de secours pour chaque interface (mode routé) ou pour l’adresse de gestion (mode transparent). L'adresse IP de secours est utilisée sur le FWSM qui est actuellement l'unité de secours. Elle doit se trouver sur le même sous-réseau que l'adresse IP active.

Voici un exemple de configuration:

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

Remarque : ne configurez pas d'adresse IP pour le lien de basculement ou pour le lien d'état (si vous allez utiliser le basculement dynamique).

Remarque : vous n'avez pas besoin d'identifier le masque de sous-réseau de l'adresse de secours. L'adresse IP et l'adresse MAC du lien de basculement ne changent pas lors du basculement. L'adresse IP active du lien de basculement accompagne toujours l'unité principale, tandis que l'adresse IP en standby accompagne l'unité secondaire.

Licences

Les unités actives et en veille doivent avoir la même licence.

Mode contextuel

Si l'unité principale est en mode contexte unique, l'unité secondaire doit également être en mode contexte unique et dans le même mode pare-feu que l'unité principale.

Si l'unité principale est en mode contexte multiple, l'unité secondaire doit également être en mode contexte multiple. Vous n'avez pas besoin de configurer le mode pare-feu des contextes de sécurité sur l'unité secondaire, car les liens de basculement et d'état résident dans le contexte système. L'unité secondaire obtient la configuration du contexte de sécurité de l'unité principale.

Remarque : la commande **mode** n'est pas répliquée sur l'unité secondaire.

Remarque : la multidiffusion n'est pas prise en charge dans le mode de contexte multiple de l'appliance de sécurité. Référez-vous à la section Fonctionnalités non prises en charge pour plus d'informations.

Configuration logicielle requise

Les deux unités d'une configuration de basculement doivent avoir la même version logicielle majeure (premier numéro) et mineure (deuxième numéro). Cependant, vous pouvez utiliser différentes versions du logiciel lors d'un processus de mise à niveau. Par exemple, vous pouvez mettre à niveau une unité de la version 3.1(1) vers la version 3.1(2) sans que le basculement ne se désactive. Cisco recommande de mettre à niveau les deux unités vers la même version pour garantir une compatibilité à long terme.

Configuration FWSM minimale pour le basculement dynamique

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 secondaire

```
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
```

Pour plus d'informations sur la façon de configurer le basculement actif et en veille, référez-vous à Configuration du basculement actif/en veille.

Configuration minimale du commutateur

- Les VLAN envoyés au FWSM principal par le Catalyst qui contient le primaire doivent correspondre aux VLAN envoyés au FWSM secondaire par le Catalyst qui contient le secondaire. (Résultat de la commande **show run | la** commande **i firewall** doit être identique.)**Châssis 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
```

Châssis secondaire

```
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
```

- Tous les VLAN envoyés doivent être présents dans la base de données VLAN et actifs.Afin d'effectuer ceci, émettez ces commandes sur le commutateur en mode de configuration :

```
vlan 10
no shut
```

Afin de vérifier si les VLAN sont dans la base de données et actifs, le résultat de la commande **show vlan** sur les deux châssis doit contenir les VLAN envoyés au FWSM et show as active.Voici est un exemple de sortie :**Châssis principal**

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

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

Châssis secondaire

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

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

- Assurez-vous que les deux FWSM ont une connectivité de couche 2 dans chaque VLAN (ils doivent se trouver dans le même sous-réseau).**Configuration requise du pare-feu transparent :**Afin d'éviter les boucles lorsque vous utilisez le basculement en mode transparent, vous devez utiliser un logiciel de commutation qui prend en charge le transfert BPDU (Bridge Protocol Data Unit). Vous devez également configurer le FWSM pour autoriser les unités BPDU. Afin d'autoriser les BPDU via le FWSM, configurez un EtherType ? ACL et l'appliquer aux deux interfaces.**Remarque :** contrairement aux plates-formes PIX et ASA, le matériel de deux lames FWSM est toujours le même, il n'y a pas de modèles ou de configurations de mémoire différents.

Dépannage

Lorsque le FWSM se recharge, les scénarios expliqués dans cette section entraîneront la désactivation du basculement.

Le module FWSM peut être rechargé pour des raisons telles qu'une panne, une réinitialisation à partir du châssis, un rechargement à partir de l'interface de ligne de commande du module FWSM, ou il peut simplement s'agir d'un nouveau module qui est inséré ou réinstallé dans un autre logement ou remis sous tension à partir du châssis.

Incompatibilité de version

Les deux unités d'une configuration de basculement doivent avoir la même version logicielle majeure (premier numéro) et mineure (deuxième numéro).

Message syslog associé : 105040

Licences incompatibles

Vous pourriez recevoir ce syslog en raison d'une licence incompatible :

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

Messages syslog associés : 105 045 et 105001

Différents modes (contexte unique ou contexte multiple)

Les modules FWSM principal et secondaire doivent être dans le même mode (simple ou multiple). Par exemple, si le principal est configuré en mode unique et le secondaire en mode multiple et que le secondaire est rechargé, les deux modules désactivent le basculement.

Principal en mode unique :

```
%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.
```

Secondaire en mode multiple (cette lame est rechargée) :

```
%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.
```

Principal en mode multiple :

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

Messages syslog associés : 105044, 103001, 105001

Deux FWSM deviennent actifs

Lorsque vous voyez ce message d'erreur dans le journal :

```
fw_create_pc_sw: fw_create_portchannel failed
```

La raison de cette erreur est que le nombre recommandé de canaux de port dans le commutateur a dépassé le maximum (128 est maximum dans la version du logiciel Cisco IOS 12.2(33)SXH4 sur Cat6000/6500). Par conséquent, la limite du bloc de descripteur d'interface (IDB) est en cours d'épuisement.

Pour cette raison, vous pourriez vous retrouver avec ces deux problèmes :

- Lorsque vous avez deux commutateurs avec des modules FWSM chacun pour agir comme actif et en veille, deux modules FWSM deviennent actifs en même temps.
- Vous ne pouvez pas créer un port-channel supplémentaire.

Afin de résoudre le problème, supprimez les ports-channel qui ne sont pas nécessaires et rechargez les FWSM.

Non-concordance VLAN

Problème

Le FWSM reçoit ce message d'erreur : **'Un partenaire actif a été détecté' 'non-concordance de configuration Vlan' 'basculement sera désactivé'**.

OU

La configuration des modules de service de pare-feu et la configuration de commutateur correspondante semblent être terminées. Cependant, les FWSM ne peuvent pas se synchroniser. Ce message est reçu sur l'hôte secondaire :

```
State check detected an Active mate

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

        No Response from Mate
```

OU

Le résultat de la commande **show failover** montre que l'état de basculement sur le module secondaire est `OFF`, l'état de basculement FWSM dans `Failover Off (pseudo-Standby)`.

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

Solution

Le problème peut être l'affectation de VLAN non correspondante sur le pare-feu (FWSM et superviseurs). Par exemple, dans l'instruction Firewall vlan-group 1, le même nombre de VLAN attribués sur chaque commutateur au pare-feu peut varier. Cela peut provoquer le problème. Si vous attribuez le même nombre de VLAN dans le pare-feu, le basculement fonctionne.

Afin d'éviter d'obtenir une erreur de non-correspondance de configuration VLAN, la sortie de commande **show vlan** doit être identique sur les deux FWSM. Ce message d'erreur se produit uniquement lorsque vous modifiez ou chargez la configuration de basculement sur le FWSM. Par exemple, lorsqu'un FWSM démarre, il charge la configuration de démarrage à partir de la mémoire flash et tente d'initialiser le basculement. À ce stade, il vérifie que les deux modules reçoivent les VLAN corrects. Si les VLAN ne correspondent pas, le message d'erreur s'affiche et le basculement reste désactivé.

Remarque : pour que le basculement fonctionne, le FWSM nécessite des configurations et des affectations de ports identiques. Il est possible d'effectuer un basculement entre les châssis, mais chaque VLAN attribué au pare-feu doit se trouver dans l'agrégation entre les deux châssis.

FWSM n'inclut aucune interface physique externe. Il utilise plutôt des interfaces VLAN. L'attribution de VLAN au FWSM est similaire à l'attribution d'un VLAN à un port de commutateur. Le FWSM inclut une interface interne vers le module de matrice de commutation (le cas échéant) ou le bus partagé. Pour plus d'informations, référez-vous à Attribution de VLAN au module de services de pare-feu.

Sachez que le mappage VLAN peut être modifié pendant une configuration FWSM en cours et échouera lors du prochain démarrage.

Le basculement est désactivé

Lorsque vous désactivez le basculement à l'aide de la commande no failover, l'état actuel de l'unité est maintenu (actif ou en veille) jusqu'à ce que l'unité soit rechargée. Elle est utilisée uniquement pour désactiver le basculement. Afin de changer l'état de l'unité de active à standby ou vice versa, vous devez utiliser la commande [no] failover active.

Informations connexes

- FWSM : Configuration du basculement
- FWSM : Messages du journal système
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.