FWSM 페일오버 문제 해결

목차

소개

이 문서에서는 FWSM(Firewall Service Module) 장애 조치 컨피그레이션의 문제를 해결하기 위해 사용할 수 있는 절차에 대해 설명합니다.

또한 이 문서에서는 장애 조치 연결 문제 해결을 시작하기 전에 시도할 수 있는 일반적인 절차의 검사 목록을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 FWSM 2.3 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

장애 조치 기능을 사용하면 스탠바이 FWSM이 실패한 FWSM의 기능을 인수할 수 있습니다. 관련된 두 FWSM은 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전, 라이센스 및 운영 모드(라우팅 또는 투명, 단일 또는 다중 컨텍스트)가 동일해야 합니다. 액티브 유닛이 실패하면 상태는 standby로 변경되며, 스탠바이 유닛은 액티브 상태로 전환됩니다. 장애 조치가 발생하면 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다.

자세한 내용은 장애 조치 사용의 장애 조치 구성 섹션을 참조하십시오.

장애 조치 체크리스트

이 체크리스트는 FWSM에서 장애 조치를 성공적으로 구성하는 데 도움이 됩니다.

- 인터페이스 확인
- 라이센스
- 컨텍스트 모드
- 소프트웨어 요구 사항
- 상태 기반 장애 조치를 위한 최소 FWSM 컨피그레이션
- 최소 스위치 구성

인터페이스 확인

FWSM의 모든 인터페이스에 구성된 대기 IP 주소가 있는지 확인합니다. 아직 구성하지 않은 경우 각 인터페이스(라우팅 모드) 또는 관리 주소(투명 모드)에 대해 액티브 및 스탠바이 IP 주소를 구성합니다. 대기 IP 주소는 현재 대기 유닛인 FWSM에서 사용됩니다. 활성 IP 주소와 동일한 서브넷에 있어야 합니다.

다음은 컨피그레이션을 보여주는 예입니다:

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

참고: 장애 조치 링크 또는 상태 링크에 대한 IP 주소를 구성하지 마십시오(상태 기반 장애 조치를 사용하려는 경우).

참고: 스탠바이 주소 서브넷 마스크를 식별할 필요는 없습니다. 장애 조치 링크 IP 주소 및 MAC 주소는 장애 조치 시 변경되지 않습니다. 장애 조치 링크의 활성 IP 주소는 항상 기본 유닛에 남아 있는 반면, 대기 IP 주소는 보조 유닛에 남아 있습니다.

라이센스

액티브 유닛과 스탠바이 유닛 모두 라이센스가 동일해야 합니다.

컨텍스트 모드

기본 유닛이 단일 컨텍스트 모드에 있을 경우, 보조 유닛도 단일 컨텍스트 모드에 있어야 하며 기본 유닛과 동일한 방화벽 모드에 있어야 합니다.

기본 유닛이 다중 컨텍스트 모드에 있을 경우 보조 유닛도 다중 컨텍스트 모드에 있어야 합니다. 장애 조치 및 상태 링크가 시스템 컨텍스트에 있으므로 보조 유닛에서 보안 컨텍스트의 방화벽 모드를 구성할 필요가 없습니다. 보조 유닛은 기본 유닛으로부터 보안 컨텍스트 컨피그레이션을 가져옵니다.

참고: mode 명령은 보조 유닛에 복제되지 않습니다.

참고: 멀티캐스트는 보안 어플라이언스의 다중 컨텍스트 모드에서 지원되지 않습니다. 자세한 내용은 지원되지 않는 기능 섹션을 참조하십시오.

소프트웨어 요구 사항

장애 조치 컨피그레이션의 두 유닛은 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 동일해야 합니다. 그러나 업그레이드 프로세스 중에 다른 버전의 소프트웨어를 사용할 수 있습니다. 예를 들어, 하나의 유닛을 버전 3.1(1)에서 버전 3.1(2)로 업그레이드하고 장애 조치를 활성 상태로 유지할 수 있습니다. Cisco에서는 장기 호환성을 위해 두 유닛을 모두 동일한 버전으로 업그레이드할 것을 권장합니다.

상태 기반 장애 조치를 위한 최소 FWSM 컨피그레이션

기본 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
```

보조 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
```

액티브 및 스탠바이 장애 조치를 구성하는 방법에 대한 자세한 내용은 액티브/스탠바이 장애 조치 구성을 참조하십시오.

최소 스위치 구성

- 기본 FWSM에 기본 FWSM을 포함하는 Catalyst가 전송한 VLAN은 보조 FWSM에 보조 FWSM을 포함하는 Catalyst가 전송한 VLAN과 일치해야 합니다. (**show run** 출력 **| 방화벽 명령**이 동일해야 합니다.)**기본 섀시**

  ```
  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
```

보조 섀시

```
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
```

- 전송되는 모든 VLAN은 VLAN 데이터베이스에 있어야 하며 활성 상태여야 합니다.이를 수행하려면 컨피그레이션 모드의 스위치에서 다음 명령을 실행합니다.

```
vlan 10
no shut
```

VLAN이 데이터베이스에 있고 활성 상태인지 확인하려면 양쪽 섀시의 **show vlan** 명령 출력에 FWSM으로 전송된 VLAN이 포함되어 있고 활성으로 표시되어야 합니다.다음은 샘플 출력입니다.**기본 섀시**

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

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

보조 섀시

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

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

- 두 FWSM이 각 VLAN에 Layer2 연결이 있는지 확인합니다(동일한 서브넷에 있어야 함).**투명한 방화벽 요구 사항:**투명 모드에서 장애 조치를 사용할 때 루프를 방지하려면 BPDU(Bridge Protocol Data Unit) 전달을 지원하는 스위치 소프트웨어를 사용해야 합니다. 또한 BPDU를 허용하도록 FWSM을 구성해야 합니다. BPDU가 FWSM을 통과하도록 허용하려면 EtherType을 구성하시겠습니까? 두 인터페이스에 모두 적용합니다.**참고:** PIX 및 ASA 플랫폼과 달리 두 FWSM 블레이드의 하드웨어는 항상 동일하며, 다른 모델이나 메모리 구성은 없습니다.

문제 해결

FWSM이 다시 로드되면 이 섹션에서 설명하는 시나리오로 인해 장애 조치가 비활성화됩니다.

FWSM은 충돌, 섀시에서 재설정, FWSM CLI에서 발급한 다시 로드와 같은 이유로 다시 로드할 수 있습니다. 또는 다른 슬롯에 삽입 또는 재장착하거나 섀시에서 전원을 공급하는 새 모듈일 수 있습니다.

버전 불일치

장애 조치 컨피그레이션의 두 유닛은 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 동일해야 합니다.

관련 syslog 메시지: 105040

호환되지 않는 라이센스

호환되지 않는 라이센스 때문에 이 syslog를 받을 수 있습니다.

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

관련 syslog 메시지: 105045 및 105001

다양한 모드(단일 및 다중 컨텍스트)

기본 FWSM과 보조 FWSM은 모두 동일한 모드(단일 또는 다중)여야 합니다. 예를 들어 기본 모드가 단일 모드로 구성되고 보조 모드가 다중 모드로 구성되어 보조 모드가 다시 로드되면 두 모듈 모두 장애 조치를 해제합니다.

단일 모드의 기본:

```
%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.
```

다중 모드의 보조(이 블레이드는 다시 로드됨):

```
%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.
```

다중 모드의 기본:

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

관련 syslog 메시지: 105044, 103001, 105001

2개의 FWSM 활성화

로그에 이 오류 메시지가 표시되면

```
fw_create_pc_sw: fw_create_portchannel failed
```

이 오류의 원인은 스위치에서 권장되는 포트 채널 수가 최대값을 초과했기 때문입니다 (Cat6000/6500의 Cisco IOS 소프트웨어 릴리스 12.2(33)SXH4에서 128개가 최대값입니다). 따라서 IDB(Interface Descriptor Block) 제한이 만료됩니다.

이로 인해 다음과 같은 두 가지 문제가 발생할 수 있습니다.

- FWSM 모듈이 각각 액티브 및 스탠바이 상태로 작동하는 두 개의 스위치가 있는 경우, 두 개의 FWSM 모듈이 동시에 액티브 상태가 됩니다.
- 추가 포트 채널을 생성할 수 없습니다.

문제 해결의 일환으로 필요하지 않은 포트 채널을 삭제하고 FWSM을 다시 로드합니다.

VLAN 불일치

문제

FWSM에 다음과 같은 오류 메시지가 표시됩니다. **'Active Mate가 감지되었습니다.' 'Vlan 컨피그레이션 불일치'** '장애 조치**가 비활성화됩니다.'**.

또는

방화벽 서비스 모듈 및 해당 스위치 컨피그레이션이 완료된 것으로 나타납니다. 그러나 FWSM은 서로 동기화할 수 없습니다. 이 메시지는 보조 호스트에서 수신됩니다.

```
State check detected an Active mate

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

        No Response from Mate
```

또는

show failover 명령의 **출력**은 보조 모듈의 장애 조치 상태가 OFF, FWSM 장애 조치 상태가 Failover Off(-) 보여줍니다.

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

솔루션

방화벽(FWSM 및 수퍼바이저) 전체에서 VLAN 할당이 일치하지 않는 것이 문제일 수 있습니다. 예를 들어, Firewall vlan-group 1 명령문에서 방화벽의 각 스위치에 할당된 동일한 VLAN 수는 다를 수 있습니다. 이로 인해 문제가 발생할 수 있습니다. 방화벽에 동일한 수의 VLAN을 할당하면 장애 조치가 작동합니다.

VLAN 컨피그레이션 불일치 오류가 발생하지 않도록 하려면 두 FWSM에서 **show** vlan 명령 출력이 동일해야 합니다. 이 오류 메시지는 FWSM에서 장애 조치 컨피그레이션을 수정하거나 로드할 때만 발생합니다. 예를 들어 FWSM이 부팅될 때 플래시에서 startup-config를 로드하고 장애 조치를 초기화하려고 시도합니다. 이때 두 모듈 모두 올바른 VLAN을 수신하는지 확인합니다. VLAN이 일치하지 않으면 오류 메시지가 표시되고 장애 조치가 비활성 상태로 유지됩니다.

참고: 장애 조치가 작동하려면 FWSM에서 동일한 컨피그레이션과 포트를 할당해야 합니다. 섀시 간 장애 조치를 수행할 수 있지만 방화벽에 할당된 각 VLAN은 두 섀시 간의 트렁크에 있어야 합니다.

FWSM에는 외부 물리적 인터페이스가 포함되어 있지 않습니다. 대신 VLAN 인터페이스를 사용합니다. FWSM에 VLAN을 할당하는 것은 스위치 포트에 VLAN을 할당하는 것과 유사합니다. FWSM에는 스위치 패브릭 모듈(있는 경우) 또는 공유 버스에 대한 내부 인터페이스가 포함되어 있습니다. 자세한 내용은 방화벽 서비스 모듈에 VLAN 할당을 참조하십시오.

VLAN 매핑은 FWSM 설정 작업 중에 수정될 수 있으며 다음 부팅 중에 실패합니다.

장애 조치가 비활성화됨

no failover 명령을 사용하여 장애 조치**를 비활성화하면 유닛**이 다시 로드될 때까지 유닛의 현재 상태(액티브 또는 스탠바이)가 유지됩니다. 이는 장애 조치를 비활성화하는 데만 사용됩니다. 유닛의 상태를 활성에서 스탠바이로 또는 그 반대로 변경하려면 **[no] failover active 명령을** 사용해야 합니다.

관련 정보

- **FWSM: 장애 조치 구성**
- **FWSM: 시스템 로그 메시지**
- **기술 지원 및 문서 – Cisco Systems**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.