



## 문제 해결

- 패킷 캡처, 1 페이지
- 네트워크 연결성 테스트, 7 페이지
- 관리 인터페이스 상태 트러블슈팅, 9 페이지
- 포트 채널 상태 확인, 10 페이지
- 소프트웨어 장애에서 복구, 12 페이지
- 손상된 파일 시스템에서 복구, 17 페이지
- 관리자 암호를 알 수 없는 경우 공장 기본 구성 복원, 27 페이지
- 트러블슈팅 로그 파일 생성, 29 페이지
- 모듈 코어 덤프 활성화, 30 페이지
- Firepower 4100/9300 새시의 일련 번호 찾기, 31 페이지
- RAID 가상 드라이브 재구성, 31 페이지
- SSD 문제 식별, 33 페이지

## 패킷 캡처

패킷 캡처는 연결 및 구성 문제를 디버깅하고 Firepower 4100/9300 새시를 통과하는 트래픽 흐름을 파악하기 위해 사용할 수 있는 매우 유용한 자산입니다. 패킷 캡처 도구를 사용하면 Firepower 4100/9300 새시의 특정 인터페이스를 통과하는 트래픽을 로깅할 수 있습니다.

여러 패킷 캡처 세션을 생성할 수 있으며, 각 세션은 여러 인터페이스의 트래픽을 캡처할 수 있습니다. 패킷 캡처 세션에 포함된 각 인터페이스에 대해 별도의 패킷 캡처(PCAP) 파일이 생성됩니다.

## 백플레인 포트 매핑

Firepower 4100/9300 새시는 내부 백플레인 포트에 다음 매핑을 사용합니다.

보안 모듈	포트 매핑	설명
보안 모듈 1/검색 엔진	Ethernet1/9	Internal-Data0/0
보안 모듈 1/검색 엔진	Ethernet1/10	Internal-Data1/0

보안 모듈	포트 매핑	설명
보안 모듈 2	Ethernet1/11	Internal-Data0/0
보안 모듈 2	Ethernet1/12	Internal-Data1/0
보안 모듈 3	Ethernet1/13	Internal-Data0/0
보안 모듈 3	Ethernet1/14	Internal-Data1/0

## 패킷 캡처 관련 지침 및 제한 사항

패킷 캡처 도구의 제한 사항은 다음과 같습니다.

- 최대 100Mbps까지만 캡처할 수 있습니다.
- 패킷 캡처 세션을 실행하기 위해 사용할 저장 공간이 충분하지 않을 경우에도 패킷 캡처 세션을 만들 수 있습니다. 패킷 캡처 세션을 시작하기 전에 저장 공간이 충분한지 확인해야 합니다.
- 싱글 와이드 4x100Gbps 또는 2x100Gbps 네트워크 모듈(각각 부품 번호 FPR-NM-4X100G 및 FPR-NM-2X100G)의 패킷 캡처 세션에서, 모듈 `adminstate`가 `off`로 설정된 경우 캡처 세션은 "Oper State Reason(상태 이유): Unknown Error(알 수 없는 오류)."로 자동으로 비활성화됩니다. 모듈 `adminstate`를 `on`으로 다시 설정한 후 캡처 세션을 다시 시작해야 합니다.  
다른 모든 네트워크 모듈을 사용하는 경우 패킷 캡처 세션은 모듈 `adminstate` 상태가 변경되는 동안 계속됩니다.
- 여러 활성 패킷 캡처 세션은 지원되지 않습니다.
- 내부 스위치의 인그레스 단계에서만 캡처합니다.
- 내부 스위치에서 이해할 수 없는 패킷(Security Group Tag 및 Network Service Header 패킷)에는 필터가 효과적이지 않습니다.
- 상위 인터페이스 하나 이상에 하위 인터페이스가 여러 개 있더라도 세션당 하위 인터페이스 하나에 대해서만 패킷을 캡처할 수 있습니다.
- EtherChannel 전체나 EtherChannel의 하위 인터페이스에 대해 패킷을 캡처할 수는 없습니다. 그러나 논리적 디바이스에 할당된 EtherChannel의 경우에는 EtherChannel의 각 멤버 인터페이스에서 패킷을 캡처할 수 있습니다. 하위 인터페이스는 할당하고 상위 인터페이스는 할당하지 않는 경우에는 멤버 인터페이스에서 패킷을 캡처할 수 없습니다.
- 캡처 세션이 활성 상태인 동안에는 PCAP 파일을 복사하거나 내보낼 수 없습니다.
- 패킷 캡처 세션을 삭제하면 해당 세션과 연결된 모든 패킷 캡처 파일도 삭제됩니다.

## 패킷 캡처 세션 생성 또는 수정

프로시저

**단계 1** **Tools(도구) > Packet Capture(패킷 캡처)**를 선택합니다.

**Capture Session(캡처 세션)** 탭에 현재 구성된 패킷 캡처 세션 목록이 표시됩니다. 현재 구성된 패킷 캡처 세션이 없는 경우 그러한 내용의 메시지가 대신 표시됩니다.

**단계 2** 다음 중 하나를 수행합니다.

- 패킷 캡처 세션을 만들려면 **Capture Session(캡처 세션)** 버튼을 클릭합니다.
- 기존 패킷 캡처 세션을 수정하려면 해당 세션의 **Edit(수정)** 버튼을 클릭합니다.

창의 왼쪽에서 특정 애플리케이션 인스턴스를 선택하면 해당 인스턴스가 표시됩니다. 이 표시는 패킷을 캡처할 인터페이스를 선택하는 데 사용됩니다. 창 오른쪽에는 패킷 캡처 세션을 정의하기 위한 필드가 있습니다.

**단계 3** 드롭다운 메뉴에서 인스턴스를 선택합니다.

**단계 4** 트래픽을 캡처할 인터페이스를 클릭합니다. 선택한 인터페이스에는 확인 표시가 나타납니다.

**단계 5** 하위 인터페이스의 경우 상위 인터페이스 왼쪽의 아이콘을 클릭하여 **Subinterface selection(하위 인터페이스 선택)** 열에서 하위 인터페이스를 확인합니다. 해당 열에서 하위 인터페이스 하나를 클릭합니다. 상위 인터페이스 하나 이상에 하위 인터페이스가 여러 개 있더라도 캡처 세션당 하위 인터페이스 하나에 대해서만 패킷을 캡처할 수 있습니다.

하위 인터페이스가 여러 개인 경우 아이콘에는 **Subinterfaces(n)(하위 인터페이스(n))** 레이블이 표시됩니다. 단일 하위 인터페이스에는 하위 인터페이스 ID가 레이블로 표시됩니다. 상위 인터페이스도 인스턴스에 할당되는 경우 상위 인터페이스나 하위 인터페이스 중 하나를 선택할 수 있으며 둘 다 선택할 수는 없습니다. 할당되지 않은 상위 인터페이스는 흐리게 표시됩니다. EtherChannel에 대한 하위 인터페이스는 지원되지 않습니다.

**단계 6** 백플레인 포트를 통해 나가는 논리적 디바이스에서 트래픽을 캡처하려면:

a) 애플리케이션 인스턴스를 나타내는 상자를 클릭합니다.

**Configure Packet Capture Session(패킷 캡처 세션 구성)** 창의 오른쪽에서 **Capture On(캡처)**, **Application Port(애플리케이션 포트)** 및 **Application Capture Direction(애플리케이션 캡처 방향)** 필드를 사용할 수 있습니다.

b) 트래픽을 캡처할 백플레인 포트를 선택하거나, **Capture On** 드롭다운 목록에서 **All Backplane Ports(모든 백플레인 포트)**를 선택합니다.

**단계 7** **Session Name(세션 이름)** 필드에 패킷 캡처 세션에 대한 이름을 입력합니다.

**단계 8** **Buffer Size(버퍼 크기)** 목록에서 미리 정의된 값 중 하나를 선택하거나 **Custom in MB(MB의 커스텀)**를 선택하고 원하는 버퍼 크기를 입력하여 이 패킷 캡처 세션을 사용하기 위한 버퍼 크기를 지정합니다. 1~2048MB 범위에서 버퍼 크기를 지정해야 합니다.

- 단계 9 캡처할 패킷의 길이를 **Snap Length**(스냅 길이) 필드에 지정합니다. 유효한 값은 64~9006바이트입니다. 기본 스냅 길이는 1518바이트입니다.
- 단계 10 이 패킷 캡처 세션이 실행될 때 기존 PCAP 파일을 덮어쓸지, 아니면 데이터를 PCAP 파일에 첨부할지를 지정합니다.
- 단계 11 애플리케이션 인스턴스와 특정 인터페이스 간 트래픽을 캡처하려면 다음을 수행합니다.
- 논리적 디바이스를 나타내는 확인란을 클릭합니다.
  - Capture On**(캡처 대상) 드롭다운 목록에서 애플리케이션 유형(예: **asa**)을 선택합니다.
  - 수신 또는 전송 트래픽을 캡처할 **Application Port**(애플리케이션 포트)를 선택합니다.
  - 논리적 디바이스로부터 지정된 인터페이스로 이동하는 트래픽만 캡처하려면 **Application Capture Direction**(애플리케이션 캡처 방향) 옆에 있는 **Egress Packets**(이그레스 패킷) 옵션을 클릭합니다.  
참고 **Egress Packets**(이그레스 패킷)을 선택하면 선택한 백플레인 포트에서만 트래픽이 캡처됩니다. 물리적 포트를 선택한 경우에도 트래픽이 캡처되지 않습니다.
  - 지정된 인터페이스에서 들어오고 나가는 트래픽을 캡처하려면 **Application Capture Direction**(애플리케이션 캡처 방향) 옆에 있는 **All Packets**(모든 패킷) 옵션을 클릭합니다.
- 단계 12 캡처되는 트래픽을 필터링하려면:
- Capture Filter**(캡처 필터) 필드에서 **Apply Filter**(필터 적용) 옵션을 클릭합니다.  
필터를 구성하기 위한 필드 집합이 표시됩니다.
  - 필터를 만들어야 하는 경우 **Create Filter**(필터 생성)를 클릭합니다.  
**Create Packet Filter**(패킷 필터 생성) 대화 상자가 나타납니다. 자세한 내용은 [패킷 캡처에 대한 필터 구성, 5 페이지](#)를 참고하십시오.
  - Apply**(적용) 드롭다운 목록에서 사용할 필터를 선택합니다.
  - To**(대상) 드롭다운 목록에서 필터를 적용할 인터페이스를 선택합니다.
  - 추가 필터를 적용하려면 **Apply Another Filter**(다른 필터 적용)를 클릭하고 위의 단계를 반복하여 추가 필터를 적용합니다.
- 단계 13 다음 중 하나를 수행합니다.
- 이 패킷 캡처 세션을 저장하고 지금 실행하려면 **Save and Run**(저장 및 실행) 버튼을 클릭합니다. 이 옵션은 현재 실행 중인 다른 패킷 캡처 세션이 없는 경우에만 사용할 수 있습니다.
  - 나중에 실행할 수 있도록 이 패킷 캡처 세션을 저장하려면 **Save**(저장) 버튼을 클릭합니다.

생성된 다른 세션과 함께 해당 세션이 **Capture Session**(캡처 세션) 탭에 나열됩니다. **Save and Run**(저장 및 실행)을 선택한 경우 패킷 캡처 세션이 패킷을 캡처합니다. 세션에서 PCAP 파일을 다운로드하려면 먼저 캡처를 중지해야 합니다.

## 패킷 캡처에 대한 필터 구성

패킷 캡처 세션에 포함된 트래픽을 제한할 필터를 만들 수 있습니다. 패킷 캡처 세션을 생성하는 동안 특정 필터를 사용해야 하는 인터페이스를 선택할 수 있습니다.



**참고** 현재 실행 중인 패킷 캡처 세션에 적용되는 필터를 수정하거나 삭제하는 경우, 해당 세션을 비활성화한 후 다시 활성화해야 변경 내용이 적용됩니다.

### 프로시저

**단계 1** **Tools(도구) > Packet Capture(패킷 캡처)**를 선택합니다.

**Capture Session(캡처 세션)** 탭에 현재 구성된 패킷 캡처 세션 목록이 표시됩니다. 현재 구성된 패킷 캡처 세션이 없는 경우 그러한 내용의 메시지가 대신 표시됩니다.

**단계 2** 다음 중 하나를 수행합니다.

- 필터를 생성하려면 **Add Filter(필터 추가)** 버튼을 클릭합니다.
- 기존 필터를 수정하려면 해당 필터의 **Edit(수정)** 버튼을 클릭합니다.

**Create or Edit Packet Filter(패킷 필터 생성 또는 수정)** 대화 상자가 나타납니다.

**단계 3** **Filter Name(필터 이름)** 필드에 패킷 캡처 필터에 대한 이름을 입력합니다.

**단계 4** 특정 프로토콜을 필터링하려면 **Protocol(프로토콜)** 목록에서 선택하거나, **Custom(커스텀)**을 선택한 다음 원하는 프로토콜을 입력합니다. 커스텀 프로토콜은 10진수 형식의 IANA 정의 프로토콜이어야 합니다(0-255).

**단계 5** 특정 EtherType을 필터링하려면 **EtherType** 목록에서 선택하거나, **Custom(커스텀)**을 선택한 다음 원하는 EtherType을 입력합니다. 커스텀 EtherType은 10진수 형식의 IANA 정의 EtherType이어야 합니다(예: IPv4 = 2048, IPv6 = 34525, ARP = 2054, SGT = 35081).

**단계 6** Inner VLAN(포트로 들어가는 동안의 VLAN ID) 또는 Outer VLAN(Firepower 4100/9300 새시에 의해 추가된 VLAN ID)을 기반으로 트래픽을 필터링하려면 지정된 필드에 VLAN ID를 입력합니다.

**단계 7** 특정 소스 또는 목적지의 트래픽을 필터링하려면 지정된 소스 또는 목적지 필드에 IP 주소와 포트를 입력하거나 MAC 주소를 입력합니다.

**참고** IPv4 또는 IPv6 주소를 사용하여 필터링할 수 있지만, 동일한 패킷 캡처 세션에서 두 주소를 모두 필터링할 수는 없습니다.

**단계 8** 필터를 저장하려면 **Save(저장)**를 클릭합니다.

생성된 다른 필터와 함께 해당 필터가 **Filter List(필터 목록)** 탭에 나열됩니다.

## 패킷 캡처 세션 시작 및 중지

프로시저

단계 1 **Tools(도구) > Packet Capture(패킷 캡처)**를 선택합니다.

**Capture Session(캡처 세션)** 탭에 현재 구성된 패킷 캡처 세션 목록이 표시됩니다. 현재 구성된 패킷 캡처 세션이 없는 경우 그러한 내용의 메시지가 대신 표시됩니다.

단계 2 패킷 캡처 세션을 시작하려면 해당 세션에 대해 **Enable Session(세션 활성화)** 버튼을 클릭한 다음 **Yes(예)**를 클릭하여 확인합니다.

참고 다른 세션이 실행 중인 동안에는 패킷 캡처 세션을 시작할 수 없습니다.

세션에 포함된 인터페이스에 대한 PCAP 파일이 트래픽 수집을 시작합니다. 세션 데이터를 덮어쓰도록 세션을 구성한 경우 기존 PCAP 데이터가 지워집니다. 아닌 경우 데이터가 기존 파일(있는 경우)에 추가됩니다.

패킷 캡처 세션이 실행 중인 동안에는 트래픽이 캡처될 때 개별 PCAP 파일의 크기가 증가합니다. 버퍼 크기 제한에 도달하면 시스템이 패킷 삭제를 시작하고 Drop Count(삭제 수) 필드가 증가합니다.

단계 3 패킷 캡처 세션을 중지하려면 해당 세션에 대해 **Disable Session(세션 비활성화)** 버튼을 클릭한 다음 **Yes(예)**를 클릭하여 확인합니다.

세션이 비활성화된 후 PCAP 파일을 다운로드할 수 있습니다([패킷 캡처 파일 다운로드](#), 6 페이지 참조).

## 패킷 캡처 파일 다운로드

네트워크 패킷 분석기를 사용하여 분석할 수 있도록 세션에서 로컬 컴퓨터로 PCAP(Packet Capture) 파일을 다운로드할 수 있습니다.

프로시저

단계 1 **Tools(도구) > Packet Capture(패킷 캡처)**를 선택합니다.

**Capture Session(캡처 세션)** 탭에 현재 구성된 패킷 캡처 세션 목록이 표시됩니다. 현재 구성된 패킷 캡처 세션이 없는 경우 그러한 내용의 메시지가 대신 표시됩니다.

단계 2 패킷 캡처 세션에서 특정 인터페이스에 대한 PCAP 파일을 다운로드하려면 인터페이스에 해당하는 **Download(다운로드)** 버튼을 클릭합니다.

참고 패킷 캡처 세션이 실행 중인 동안에는 PCAP 파일을 다운로드할 수 없습니다.

브라우저에 따라, 지정된 PCAP 파일이 기본 다운로드 위치에 자동으로 다운로드되거나 파일을 저장하라는 프롬프트가 표시됩니다.

## 패킷 캡처 세션 삭제

현재 실행하고 있지 않은 개별 패킷 캡처 세션을 삭제하거나, 모든 비활성 패킷 캡처 세션을 삭제할 수 있습니다.

프로시저

**단계 1** **Tools(도구) > Packet Capture(패킷 캡처)**를 선택합니다.

**Capture Session(캡처 세션)** 탭에 현재 구성된 패킷 캡처 세션 목록이 표시됩니다. 현재 구성된 패킷 캡처 세션이 없는 경우 그러한 내용의 메시지가 대신 표시됩니다.

**단계 2** 특정 패킷 캡처 세션을 삭제하려면 세션에 해당하는 **Delete(삭제)** 버튼을 클릭합니다.

**단계 3** 모든 비활성 패킷 캡처 세션을 삭제하려면 패킷 캡처 세션 목록 위에 있는 **Delete All Sessions(모든 세션 삭제)** 버튼을 클릭합니다.

## 네트워크 연결성 테스트

시작하기 전에

호스트 이름 또는 IPv4 주소가 있는 네트워크에서 다른 디바이스를 ping하여 기본 네트워크 연결을 테스트하려면 **ping** 명령을 사용합니다. 호스트 이름 또는 IPv6 주소가 있는 네트워크에서 다른 디바이스를 ping하려면 **ping6** 명령을 사용합니다.

호스트 이름 또는 IPv4 주소를 사용하는 네트워크에서 다른 디바이스에 대한 경로를 추적하려면 **tracert** 명령을 사용합니다. 호스트 이름 또는 IPv6 주소를 사용하는 네트워크에서 다른 디바이스에 대한 경로를 추적하려면 **tracert6** 명령을 사용합니다.

- **ping** 및 **ping6** 명령은 `local-mgmt` 모드에서 사용할 수 있습니다.
- **ping** 명령은 `module` 모드에서도 사용할 수 있습니다.
- **tracert** 및 **tracert6** 명령은 `local-mgmt` 모드에서 사용할 수 있습니다.
- **tracert** 명령은 `module` 모드에서도 사용할 수 있습니다.

## 프로시저

단계 1 다음 명령 중 하나를 입력하여 `local-mgmt` 또는 `module` 모드에 연결합니다.

- `connect local-mgmt`
- `connect module module-ID {console | telnet}`

예제:

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

단계 2 호스트 이름 또는 IPv4 주소를 사용하는 네트워크에서 다른 디바이스를 ping하여 기본 네트워크 연결을 테스트합니다.

`ping {hostname | IPv4_address} [count number_packets ] | [deadline seconds ] | [interval seconds ] | [packet-size bytes ]`

예제:

이 예에서는 네트워크에 있는 다른 디바이스를 12번 ping하여 연결하는 방법을 보여 줍니다.

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

단계 3 호스트 이름 또는 IPv4 주소를 사용하는 네트워크에서 다른 디바이스에 대한 경로를 추적하려면 다음을 수행합니다.

`traceroute {hostname | IPv4_address}`

예제:

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1 198.51.100.57 (198.51.100.57) 0.640 ms 0.737 ms 0.686 ms
 2 net1-gw1-13.cisco.com (198.51.100.101) 2.050 ms 2.038 ms 2.028 ms
 3 net1-sec-gw2.cisco.com (198.51.100.201) 0.540 ms 0.591 ms 0.577 ms
 4 net1-fp9300-19.cisco.com (198.51.100.108) 0.336 ms 0.267 ms 0.289 ms
```



```
FP9300-A(local-mgmt)#
```

단계 4 (선택 사항) **exit**를 입력하여 `local-mgmt` 모드를 종료하고 최상위 레벨 모드로 돌아갑니다.

## 관리 인터페이스 상태 트러블슈팅

초기화 및 구성 중에 관리 인터페이스가 작동하지 않는 것으로 의심되는 경우(예: 새시 관리자에 액세스할 수 없음) `local-mgmt` 셸의 **show mgmt-port** 명령을 사용하여 관리 인터페이스의 상태를 확인합니다.



참고 `fxos` 셸에서는 현재 잘못된 정보를 표시하므로 **show interface brief** 명령을 사용하지 마십시오.

프로시저

단계 1 다음 명령 중 하나를 입력하여 `local-mgmt` 모드에 연결합니다.

- **connect local-mgmt**

예제:

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

단계 2 **show mgmt-port** 명령을 사용하여 관리 인터페이스의 상태를 확인합니다.

예제:

```
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14 Bcast:10.89.5.63 Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:3210912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:705434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1648941394 (1.5 GiB) TX bytes:138386379 (131.9 MiB)

firepower(local-mgmt)#
```

**show mgmt-ip-debug** 명령을 사용할 수도 있습니다. 그러나 인터페이스 구성 정보의 광범위 한 목록을 생성합니다.

## 포트 채널 상태 확인

다음 단계를 수행하여 현재 정의된 포트 채널의 상태를 확인할 수 있습니다.

프로시저

**단계 1** 다음 명령을 입력하여 /eth-uplink/fabric 모드를 시작합니다.

- **scope eth-uplink**
- **scope fabric {a | b}**

예제:

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

**단계 2** **show port-channel** 명령을 입력하여 각각의 관리 상태 및 작동 상태와 함께 현재 포트 채널 목록을 표시합니다.

예제:

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State          State Reason
  -----
  10                    Port-channel10 Data            Enabl
ed   Failed                No operational members
  11                    Port-channel11 Data            Enabl
ed   Failed                No operational members
  12                    Port-channel12 Data            Disab
led  Admin Down             Administratively down
  48                    Port-channel48 Cluster          Enabl
ed   Up

FP9300-A /eth-uplink/fabric #
```

**단계 3** 다음 명령을 입력하여 /port-channel 모드를 시작하고 개별 포트 채널 및 포트 정보를 표시합니다.

- **scope port-channel ID**

예제:

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
```

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under

```
license.
<--- remaining lines removed for brevity --->
FP9300-A (fxos) #
```

단계 4 **show** 명령을 입력하여 지정된 포트 채널에 대한 상태 정보를 표시합니다.

예제:

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State          State Reason
  -----
  10                        Port-channel10 Data          Enabl
ed      Failed                No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

단계 5 **show member-port** 명령을 입력하여 포트 채널의 멤버 포트에 대한 상태 정보를 표시합니다.

예제:

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
  Port Name          Membership      Oper State      State Reas
on
  -----
  Ethernet2/3        Suspended      Failed          Suspended
  Ethernet2/4        Suspended      Failed          Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

포트 채널은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. 포트 채널을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, 포트 채널은 일시 중단 상태로 전환됩니다.

단계 6 추가 포트 채널 및 LACP 정보를 보려면 `/eth-uplink/fabric/port-channel` 모드를 종료하고 다음 명령을 입력하여 `fxos` 모드를 시작합니다.

- **top**
- **connect fxos**

예제:

단계 7 **show port-channel summary** 명령을 입력하여 현재 포트 채널에 대한 요약 정보를 표시합니다.

예제:

```
FP9300-A (fxos) # show port-channel summary
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
```

```

M - Not in use. Min-links not met
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
10    Po10 (SD)  Eth       LACP      Eth2/3 (s)  Eth2/4 (s)
11    Po11 (SD)  Eth       LACP      Eth2/1 (s)  Eth2/2 (s)
12    Po12 (SD)  Eth       LACP      Eth1/4 (D)  Eth1/5 (D)
48    Po48 (SU)  Eth       LACP      Eth1/1 (P)  Eth1/2 (P)

```

추가 **show port-channel** 및 **show lacp** 명령은 `fxos` 모드에서 사용할 수 있습니다. 이러한 명령은 다양한 포트 채널 및 용량, 트래픽, 카운터, 사용량 등의 LACP 정보를 표시하는 데 사용할 수 있습니다.

다음에 수행할 작업

포트 채널 생성 관련 정보는 [EtherChannel\(포트 채널\) 추가](#)의 내용을 참조하십시오.

## 소프트웨어 장애에서 복구

시작하기 전에

시스템의 성공적인 부팅을 방해하는 소프트웨어 장애가 발생하면 다음 절차에 따라 소프트웨어의 새 버전을 부팅할 수 있습니다. 이 프로세스를 완료하려면 kickstart 이미지를 TFTP 부팅하고, 새 시스템과 관리자 이미지를 다운로드하고, 새 이미지를 사용하여 부팅해야 합니다.

Cisco.com의 다음 위치에서 특정 FXOS 버전에 대한 복구 이미지를 가져올 수 있습니다.

- Firepower 9300—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 Series—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

복구 이미지에는 세 개의 별도 파일이 포함되어 있습니다. 예를 들어 다음은 FXOS 2.1.1.64의 현재 복구 이미지입니다.

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

## 프로시저

단계 1 ROMMON에 액세스합니다.

- a) 콘솔 포트에 연결합니다.
- b) 시스템을 재부팅합니다.

시스템이 로딩을 시작하며, 로딩 프로세스 중에 카운트다운 타이머가 표시됩니다.

- c) 카운트다운 중에 **Escape** 키를 눌러 ROMMON 모드로 들어갑니다.

예제:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
```

```
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

단계 2 킥스타트 이미지를 TFTP 부팅합니다.

- a) 관리 IP 주소, 관리 넷마스크, 게이트웨이 IP 주소가 올바르게 설정되었는지 확인합니다. **set** 명령을 사용하여 해당 값을 볼 수 있습니다. **ping** 명령을 사용하여 TFTP 서버에 대한 연결을 테스트할 수 있습니다.

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) 킥스타트 이미지를 Firepower 4100/9300 새시에서 액세스 가능한 TFTP 디렉터리에 복사합니다.

참고 킥스타트 이미지 버전 번호는 번들 버전 번호와 일치하지 않습니다. Cisco.com 소프트웨어 다운로드 페이지에서 FXOS 버전과 킥스타트 이미지 간 매핑을 보여주는 정보를 찾을 수 있습니다.

- c) boot 명령을 사용하여 ROMMON에서 이미지를 부팅합니다.

```
boot tftp://<IP address>/<path to image>
```

참고 Firepower 4100/9300 새시의 전면 패널에 있는 USB 슬롯에 삽입한 USB 미디어 디바이스를 사용하여 ROMMON에서 키스타트를 부팅할 수도 있습니다. 시스템이 실행 중일 때 USB 디바이스를 삽입하는 경우 시스템을 리부팅해야 USB 디바이스가 인식됩니다.

이미지가 수신 중임을 나타내는 일련의 # 표시가 나타난 다음 키스타트 이미지가 로드됩니다.

예제:

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

**단계 3** Firepower 4100/9300 새시에 방금 로드한 키스타트 이미지와 일치하는 복구 시스템 및 관리자 이미지를 다운로드합니다.

- a) 복구 시스템 및 관리자 이미지를 다운로드하려면 관리 IP 주소 및 게이트웨이를 설정해야 합니다. USB를 통해 이러한 이미지를 다운로드할 수 없습니다.

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
```

```
switch(boot) (config) # exit
```

- b) 원격 서버에서 bootflash로 복구 시스템 및 관리자 이미지를 복사합니다.

```
switch(boot)# copy URL bootflash:
```

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp://username@hostname/path/image\_name**
- **scp://username@hostname/path/image\_name**
- **sftp://username@hostname/path/image\_name**
- **tftp://hostname/path/image\_name**

예제:

```
switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
```

```
switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
```

- c) 이미지를 성공적으로 Firepower 4100/9300 새시에 복사한 후 `nuova-sim-mgmt-nsg.0.1.0.001.bin`에서 관리자 이미지로 symlink를 만듭니다. 이 링크는 로드할 관리자 이미지를 로드 메커니즘에 알려줍니다. 어떤 이미지를 로드하려고 하는지와 상관없이 symlink 이름은 항상 `nuova-sim-mgmt-nsg.0.1.0.001.bin`이어야 합니다.

```
switch(boot) # copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

예제:

```
switch(boot) # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(boot) (config) # interface mgmt 0
switch(boot) (config-if) # ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if) # no shutdown
switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway 10.0.0.1
switch(boot) (config) # exit
switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
Trying to connect to tftp server.....
```

```

Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#

```

**단계 4** 방금 다운로드한 시스템 이미지를 로드합니다.

```
switch(boot)# load bootflash:<system-image>
```

예제:

```

switch(boot)# load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful
...
System is coming up ... Please wait ...

Cisco FPR Series Security Appliance
FP9300-A login:

```

**단계 5** 시스템이 이전 이미지를 로드하려고 시도하지 못하게 하려면, 복구 이미지를 로드한 후 다음 명령을 입력합니다.

참고 이 단계는 복구 이미지를 로드한 직후 수행해야 합니다.

```

FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
FP9300-A /org/fw-platform-pack* # commit-buffer

```

**단계 6** Firepower 4100/9300 새시에서 사용할 플랫폼 번들 이미지를 다운로드 및 설치합니다. 자세한 내용은 [이미지 관리](#)를 참고하십시오.

예제:

```

FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
           Tftp      192.168.1.2          0          Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active

```



Time Stamp: 2012-01-01T07:40:28.000  
 Build Date: 2017-02-28 13:51:08 UTC  
 FP9300-A /firmware #

## 손상된 파일 시스템에서 복구

시작하기 전에

Supervisor의 온보드 플래시가 손상되고 시스템을 더 이상 성공적으로 시작할 수 없는 경우 다음 절차를 사용하여 시스템을 복구할 수 있습니다. 이 프로세스를 완료하려면 kickstart 이미지를 TFTP 부팅하고, 플래시를 재포맷하고, 새 시스템과 관리자 이미지를 다운로드하고, 새 이미지를 사용하여 부팅해야 합니다.



참고 이 절차에는 시스템 플래시 재포맷이 포함됩니다. 그 결과, 시스템이 복구된 후 완전히 다시 구성해야 합니다.

Cisco.com의 다음 위치에서 특정 FXOS 버전에 대한 복구 이미지를 가져올 수 있습니다.

- Firepower 9300—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 Series—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

복구 이미지에는 세 개의 별도 파일이 포함되어 있습니다. 예를 들어 다음은 FXOS 2.1.1.64의 복구 이미지입니다.

Recovery image (kickstart) for FX-OS 2.1.1.64.  
 fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.  
 fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.  
 fxos-k9-system.5.0.3.N2.4.11.63.SPA

프로시저

단계 1 ROMMON에 액세스합니다.

- a) 콘솔 포트에 연결합니다.
- b) 시스템을 재부팅합니다.

시스템이 로딩을 시작하며, 로딩 프로세스 중에 카운트다운 타이머가 표시됩니다.

- c) 카운트다운 중에 **Escape** 키를 눌러 ROMMON 모드로 들어갑니다.

## 예제:

```

Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 >

```

## 단계 2 킥스타트 이미지를 TFTP 부팅합니다.

- a) 관리 IP 주소, 관리 넷마스크, 게이트웨이 IP 주소가 올바르게 설정되었는지 확인합니다. **set** 명령을 사용하여 해당 값을 볼 수 있습니다. **ping** 명령을 사용하여 TFTP 서버에 대한 연결을 테스트할 수 있습니다.

```

rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>

```

- b) 킥스타트 이미지를 Firepower 4100/9300 새시에서 액세스 가능한 TFTP 디렉터리에 복사합니다.
- 참고 킥스타트 이미지 버전 번호는 번들 버전 번호와 일치하지 않습니다. Cisco.com 소프트웨어 다운로드 페이지에서 FXOS 버전과 킥스타트 이미지 간 매핑을 보여주는 정보를 찾을 수 있습니다.
- c) boot 명령을 사용하여 ROMMON에서 이미지를 부팅합니다.

```
boot tftp://<IP address>/<path to image>
```

참고 Firepower 4100/9300 새시의 전면 패널에 있는 USB 슬롯에 삽입한 USB 미디어 디바이스를 사용하여 ROMMON에서 킥스타트를 부팅할 수도 있습니다. 시스템이 실행 중일 때 USB 디바이스를 삽입하는 경우 시스템을 리부팅해야 USB 디바이스가 인식됩니다.

이미지가 수신 중임을 나타내는 일련의 # 표시가 나타난 다음 킥스타트 이미지가 로드됩니다.

예제:

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

**단계 3** 킥스타트 이미지가 로드된 후 **init system** 명령을 사용하여 플래시를 재포맷합니다.

**init system** 명령은 시스템에 다운로드된 모든 소프트웨어 이미지 및 시스템의 모든 구성을 포함하여 플래시의 콘텐츠를 지웁니다. 이 명령을 완료하는 데 약 20~30분 정도 소요됩니다.

예제:

```
switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:

Do you want to continue? (y/n) [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
```

```

Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Sysdebug partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done

```

단계 4 복구 이미지를 Firepower 4100/9300 새시에 다운로드합니다.

- a) 복구 이미지를 다운로드하려면 관리 IP 주소 및 게이트웨이를 설정해야 합니다. USB를 통해 이러한 이미지를 다운로드할 수 없습니다.

```

switch(boot)# config terminal
switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address <ip address> <netmask>
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway <gateway>
switch(boot) (config)# exit

```

- b) 원격 서버에서 bootflash로 복구 이미지 세 개를 모두 복사합니다.

```
switch(boot)# copy URL bootflash:
```

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp://username@hostname/path/image\_name**
- **scp://username@hostname/path/image\_name**
- **sftp://username@hostname/path/image\_name**
- **tftp://hostname/path/image\_name**

예제:

```

switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:

```

```

switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:

```

```

switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:

```

- c) 이미지를 성공적으로 Firepower 4100/9300 새시에 복사한 후 `nuova-sim-mgmt-nsg.0.1.0.001.bin`에서 관리자 이미지로 symlink를 만듭니다. 이 링크는 로드할 관리자 이미지를 로드 메커니즘에 알려줍니다. 어떤 이미지를 로드하려고 하는지와 상관없이 symlink 이름은 항상 `nuova-sim-mgmt-nsg.0.1.0.001.bin`이어야 합니다.

```
switch(boot)# copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

예제:

```
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.

switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway 10.0.0.1
switch(boot) (config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

단계 5 스위치를 로드합니다.

```
switch(boot)# reload
```

예제:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.
```

```
!! Rommon image verified successfully !!
```

```

Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb

autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 >

```

## 단계 6 키스타트 및 시스템 이미지에서 부팅합니다.

```
rommon 1 > boot <kickstart-image> <system-image>
```

**참고** 시스템 이미지가 로드되는 동안 라이선스 관리자 실패 메시지가 표시됩니다. 이러한 메시지는 안전하게 무시할 수 있습니다.

### 예제:

```

rommon 1 > dir
Directory of: bootflash:\

01/01/12 12:33a <DIR>          4,096 .
01/01/12 12:33a <DIR>          4,096 ..
01/01/12 12:16a <DIR>          16,384 lost+found
01/01/12 12:27a              34,333,696 fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
01/01/12 12:29a              330,646,465 fxos-k9-manager.4.1.1.69.SPA
01/01/12 12:31a              250,643,172 fxos-k9-system.5.0.3.N2.4.11.69.SPA
01/01/12 12:34a              330,646,465 nuova-sim-mgmt-nsg.0.1.0.001.bin
      4 File(s) 946,269,798 bytes
      3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan 1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed

```

```
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA
```

```
Manager image digital signature verification successful
```

```
...
```

```
System is coming up ... Please wait ...
nohup: appending output to `nohup.out'
```

```
---- Basic System Configuration Dialog ----
```

```
This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the Fabric interconnect and its clustering mode is performed through these steps.
```

```
Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.
```

```
You have chosen to setup a new Security Appliance. Continue? (y/n):
```

**단계 7** 이미지가 로드되면 초기 구성 설정을 입력하라는 프롬프트가 표시됩니다. 자세한 내용은 [콘솔 포트를 사용한 초기 구성](#)을 참고하십시오.

**단계 8** Firepower 4100/9300 새시에서 사용할 플랫폼 번들 이미지를 다운로드합니다. 자세한 내용은 [이미지 관리](#)를 참조하십시오.

예제:

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port    Userid    State
  -----
  fxos-k9.2.1.1.73.SPA
      Tftp    192.168.1.2          0
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
  Time Stamp: 2012-01-01T07:40:28.000
  Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

**단계 9** 이전 단계에서 다운로드한 플랫폼 번들 이미지를 설치합니다.

참고 설치 프로세스는 일반적으로 15~20분 정도 소요됩니다.

a) 자동 설치 모드를 입력합니다.

```
Firepower-chassis /firmware # scope auto-install
```

b) FXOS 플랫폼 번들을 설치합니다.

```
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number
```

*version\_number*는 설치 중인 FXOS 플랫폼 번들의 버전 번호입니다(예: 2.1(1.73)).

- c) 시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

**yes**를 입력하여 검증을 계속할 것인지 확인합니다.

- d) **yes**를 입력하여 설치를 계속할 것인지 확인하거나 **no**를 입력하여 설치를 취소합니다.

FXOS에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

- e) 업그레이드 프로세스를 모니터링하려면 다음과 같이 합니다.

- **scope firmware**을 입력합니다.
- **scope auto-install**을 입력합니다.
- **show fsm status expand**을 입력합니다.

예:

```
TB10 /firmware/auto-install # show fsm status expand
```

```
FSM Status:
  Affected Object: sys/fw-system/fsm
  Current FSM: Deploy
  Status: In Progress
  Completion Time:
  Progress (%): 98

FSM Stage:
Order  Stage Name                                     Status      Try
-----
1      DeployWaitForDeploy                               Success     0
2      DeployResolveDistributableNames                   Skip        0
3      DeployResolveDistributable                         Skip        0
4      DeployResolveImages                                Skip        0
5      DeployValidatePlatformPack                         Success     1
6      DeployDebundlePort                                 Success     0
7      DeployPollDebundlePort                             Success     1
8      DeployActivateUCSM                                 Success     0
9      DeployPollActivateOfUCSM                           Success     0
10     DeployActivateMgmtExt                               Skip        0
11     DeployPollActivateOfMgmtExt                         Skip        0
12     DeployUpdateIOM                                    Skip        0
13     DeployPollUpdateOfIOM                              Skip        0
14     DeployActivateIOM                                  Skip        0
15     DeployPollActivateOfIOM                            Skip        0
16     DeployActivateRemoteFI                             Skip        0
17     DeployPollActivateOfRemoteFI                       Skip        0
18     DeployWaitForUserAck                               Skip        0
19     DeployActivateLocalFI                              Success     0
20     DeployPollActivateOfLocalFI                        In Progress 1
```

- 참고     단계의 상태가 "In Progress(진행 중)"에서 "Skip(건너뛰기)" 또는 "Success(성공)"로 변경될 때까지 다음 단계로 진행하지 마십시오.



**단계 10** 시스템 복구에 사용한 이미지에 맞는 플랫폼 번들 이미지가 설치되어 있는 경우, 나중에 시스템을 로드할 때 사용할 수 있도록 수동으로 키스타트 및 시스템 이미지를 활성화해야 합니다. 사용된 복구 이미지와 동일한 이미지가 있는 플랫폼 번들을 설치하는 경우 자동 활성화가 적용되지 않습니다.

a) 패브릭 인터커넥트 a의 범위를 설정합니다.

```
FP9300-A# scope fabric-interconnect a
```

b) 실행 중인 커널 버전 및 실행 중인 시스템 버전을 보려면 **show version** 명령을 사용합니다. 이러한 문자열을 사용하여 이미지를 활성화합니다.

```
FP9300-A /fabric-interconnect # show version
```

**참고** Startup-Kern-Vers 및 Startup-Sys-Vers가 이미 설정되어 있고 Running-Kern-Vers 및 Running-Sys-Vers와 일치하는 경우, 이미지를 활성화할 필요가 없으며 11단계를 진행할 수 있습니다.

c) 다음 명령을 입력하여 이미지를 활성화합니다.

```
FP9300-A /fabric-interconnect # activate firmware
kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

**참고** 서버 상태가 "Disk Failed(디스크 실패)"로 변경될 수 있습니다. 이 메시지에 대해 걱정할 필요가 없으며 이 절차를 계속 진행할 수 있습니다.

d) 시작 버전이 올바르게 설정되었는지 확인하고 이미지의 활성화 상태를 모니터링하려면 **show version** 명령을 사용합니다.

**중요** 상태가 "Activating(활성)"에서 "Ready(준비)"로 변경될 때까지 다음 단계로 진행하지 마십시오.

```
FP9300-A /fabric-interconnect # show version
```

**예제:**

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers:
  Startup-Sys-Vers:
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
```

```

Running-Kern-Vers: 5.0(3)N2(4.11.69)
Running-Sys-Vers: 5.0(3)N2(4.11.69)
Package-Vers: 2.1(1.73)
Startup-Kern-Vers: 5.0(3)N2(4.11.69)
Startup-Sys-Vers: 5.0(3)N2(4.11.69)
Act-Kern-Status: Activating
Act-Sys-Status: Activating
Bootloader-Vers:

```

```

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

```

단계 11 시스템을 재부팅합니다.

예제:

```

FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #

```

시스템은 각 보안 모듈/엔진의 전원을 끈 다음 마지막으로 Firepower 4100/9300 채시의 전원을 끄고 재시작합니다. 이 프로세스는 약 5~10분 정도 걸립니다.

단계 12 시스템 상태를 모니터링합니다. 서버 상태가 "Discovery(검색)"에서 "Config(구성)"로 바뀐 다음 마지막으로 "Ok"로 바뀝니다.

예제:

```

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Discovery In Progress
1/2 Equipped Discovery In Progress
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Config Complete
1/2 Equipped Config Complete
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Ok Complete
1/2 Equipped Ok Complete
1/3 Empty

```

Overall Status(전체 상태)가 "Ok"이면 시스템이 복구된 것입니다. 여전히 보안 어플라이언스를 재구성하고(라이선스 구성 포함) 논리적 디바이스를 다시 생성해야 합니다. 자세한 내용:

- Firepower 9300 빠른 시작 가이드—<http://www.cisco.com/go/firepower9300-quick>
- Firepower 9300 환경 설정 가이드—<http://www.cisco.com/go/firepower9300-config>
- Firepower 4100 Series 빠른 시작 가이드—<http://www.cisco.com/go/firepower4100-quick>
- Firepower 4100 Series 환경 설정 가이드—<http://www.cisco.com/go/firepower4100-config>

## 관리자 암호를 알 수 없는 경우 공장 기본 구성 복원

이 절차에서는 Firepower 4100/9300 새시 시스템을 관리자 비밀번호를 포함한 기본 구성 설정으로 되돌립니다. 관리자 비밀번호를 알 수 없는 경우 이 절차를 사용하여 디바이스에서 구성을 재설정합니다. 이 절차를 수행하면 설치된 모든 논리적 디바이스도 지워집니다.



**참고** 이 절차를 수행하려면 Firepower 4100/9300 새시에 대한 콘솔 액세스가 필요합니다.

### 프로시저

**단계 1** 제공된 콘솔 케이블을 사용하여 컴퓨터를 콘솔 포트에 연결하고, 9600 baud, 8 data bit, 패리티 없음, 1 stop bit, flow control 없음으로 설정된 터미널 에뮬레이터를 사용하여 콘솔에 연결합니다. 콘솔 케이블에 대한 자세한 내용은 [Cisco Firepower 9300 하드웨어 설치 가이드](#)를 참조하십시오.

**단계 2** 디바이스 전원을 켭니다. 다음 프롬프트가 표시되면 ESC를 눌러 부팅을 중지합니다.

예제:

```
!! Rommon image verified successfully !!
```

```
Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
```

```
Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: 00:00:00:00:00:00
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
```

```
Boot interrupted.
rommon 1 >
```

단계 3 키스타트 및 시스템 이미지 이름을 기록합니다.

예제:

```
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

단계 4 키스타트 이미지를 로드합니다.

```
rommon 1 > boot kickstart_image
```

예제:

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
can't create lock file /var/lock/mtab~302: No such file or directory (use -n flag to override)
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

단계 5 config terminal 모드를 시작합니다.

```
switch(boot) # config terminal
```

예제:

```
switch(boot)#
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

단계 6 비밀번호를 재설정하고 변경 사항을 확인합니다.

```
switch(boot) (config) # admin-password erase
```

참고 이 단계에서는 모든 구성을 지우고 시스템을 기본 구성 설정으로 되돌립니다.

예제:

```
switch(boot) (config) # admin-password erase
Your password and configuration will be erased!
Do you want to continue? (y/n) [n] y
```

단계 7 config terminal 모드를 종료합니다.

```
switch(boot) (config) # exit
```

단계 8 이 절차의 3단계에서 기록한 시스템 이미지를 로드하고 초기 구성 작업 플로우를 사용하여 시스템을 처음부터 구성합니다.

```
switch(boot) # load system_image
```

예제:

```
switch(boot) # load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

```
Uncompressing system image: bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

## 트러블슈팅 로그 파일 생성

로그 파일을 생성하여 트러블슈팅에 도움을 주거나, 요청을 받은 경우 Cisco TAC에 전송할 수 있습니다.

프로시저

단계 1 **Tools(도구) > Troubleshooting Logs(트러블슈팅 로그)**를 선택합니다.

단계 2 드롭다운 목록에서 생성하려는 로그 파일 유형을 선택합니다.

- 새시 - 수퍼바이저 및 서비스 매니저를 비롯하여 새시 문제 및 소프트웨어 문제를 트러블슈팅하는 데 사용할 로그 파일을 생성합니다.
- 모듈 <#> - 보안 모듈/엔진 문제를 트러블슈팅하는 데 사용할 로그 파일을 생성합니다.

단계 3 **Generate Log(로그 생성)**를 클릭합니다.

단계 4 **Yes(예)**를 클릭하여 로그 파일을 생성할 것을 확인합니다.

로그 파일이 생성됩니다. 이 프로세스는 시간이 걸릴 수 있습니다. 로그 파일을 생성하는 동안 노란색 상태 메시지가 표시됩니다. 로그 파일 생성을 취소하려면 상태 메시지에서 **Abort Job(작업 중단)**을 클릭하면 됩니다. 로그 파일이 생성되고 나면, 상태 메시지가 녹색으로 변경되어 작업이 성공적으로 완료되었음을 나타냅니다.

단계 5 생성된 로그 파일을 다운로드하려면 **Download Files(파일 다운로드)** 목록에서 로그 파일을 찾은 다음, **Download(다운로드)**를 클릭합니다. 로그 파일은 techsupport 폴더 아래에 저장됩니다.

참고 새로 생성된 파일이 **Download Files(파일 다운로드)** 목록에 표시되도록 **Refresh(새로 고침)**을 클릭해야 할 수 있습니다.

단계 6 생성된 로그 파일을 삭제하려면 **Download Files(파일 다운로드)** 목록에서 로그 파일을 찾은 다음, **Delete(삭제)**를 클릭합니다.

## 모듈 코어 덤프 활성화

모듈에서 코어 덤프를 활성화하면 시스템 충돌 시 트러블슈팅에 도움이 되거나, 요청 시 Cisco TAC 로 전송할 수 있습니다.

프로시저

단계 1 원하는 모듈에 연결합니다. 예:

```
Firepower# connect module 1 console
```

단계 2 (선택 사항) 다음 명령을 입력하여 현재 코어 덤프 상태를 확인합니다.

```
Firepower-module1> show coredump detail
```

명령 출력에는 코어 덤프 압축의 활성화 여부를 포함하여 현재 코어 덤프 상태 정보가 표시 됩니다.

예제:

```
Firepower-module1>show coredump detail
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

참고 이 명령은 어플라이언스에서 ASA 논리적 디바이스를 실행하는 경우에만 사용할 수 있으며, 어플라이언스에서 FTD 논리적 디바이스를 실행할 때는 사용할 수 없습니다.

단계 3 **config coredump** 명령을 사용하여 코어 덤프를 활성화 또는 비활성화하고, 충돌 중에 코어 덤프 압축을 활성화 또는 비활성화합니다.

- **config coredump enable** 을 사용하여 충돌 중에 코어 덤프 생성을 활성화합니다.
- **config coredump disable** 을 사용하여 충돌 중에 코어 덤프 생성을 비활성화합니다.
- **config coredump compress enable** 을 사용하여 코어 덤프의 압축을 활성화합니다.
- **config coredump compress disable** 을 사용하여 코어 덤프 압축을 비활성화합니다.

예제:

```
Firepower-module1>config coredump enable
Coredump enabled successfully.
ASA coredump enabled, do 'config coredump disableAsa' to disable
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system
failure. Are you sure? (y/n):
y
Firepower-module1>
```

참고 코어 덤프 파일은 디스크 공간을 사용하며, 공간이 부족하고 압축이 활성화되지 않은 경우 코어 덤프가 활성화된 경우에도 코어 덤프 파일이 저장되지 않을 수 있습니다.

## Firepower 4100/9300 새시의 일련 번호 찾기

Firepower 4100/9300 새시 및 일련 번호에 대한 세부 정보를 찾을 수 있습니다. Firepower 4100/9300 새시의 일련 번호는 논리적 디바이스의 일련 번호와 다릅니다.

프로시저

단계 1 **Overview > Inventory > All**을 선택합니다.

이 표에서는 새시에 설치된 구성 요소를 나열하고 해당 구성 요소에 대한 관련 세부 정보를 제공합니다.

단계 2 **Serial** 열에서 새시 일련번호를 찾으십시오.

## RAID 가상 드라이브 재구성

RAID(Redundant Array of Independent Disks)는 고성능과 내결함성(fault tolerance)을 제공하는 여러 독립적인 실제 드라이브로 구성된 어레이 또는 그룹입니다. 드라이브 그룹은 실제 드라이브의 그룹입니다. 이러한 드라이브는 가상 드라이브로 알려진 파티션으로 관리됩니다.

RAID 드라이브 그룹은 단일 드라이브 스토리지 시스템보다 데이터 스토리지 안정성과 내결함성을 더욱 개선합니다. 나머지 드라이브에서 누락된 데이터를 재구성하여 드라이브 장애로 인한 데이터 손실을 방지할 수 있습니다. RAID는 I/O 성능을 개선하고 스토리지 하위 시스템의 안정성을 향상합니다.

RAID 드라이브 중 하나에 장애가 발생했거나 오프라인인 경우 RAID 가상 드라이브는 성능이 저하된 상태로 간주됩니다. 이 절차를 사용하여 RAID 가상 드라이브가 성능이 저하된 상태인지 확인하고, 일시적으로 로컬 디스크 구성 보호 정책을 no로 설정하여 필요한 경우 재구축합니다.



참고 로컬 디스크 구성 보호 정책을 no로 설정하면 디스크의 모든 데이터가 삭제됩니다.

프로시저

단계 1 RAID 상태를 확인합니다.

1. 새시 모드로 들어갑니다.

**scope chassis**

2. 서버 모드를 활성화합니다.

**scope server 1**

3. RAID 컨트롤러를 입력합니다.

**scope raid-controller 1 sas**

4. 가상 드라이브를 봅니다.

**show virtual-drive**

RAID 가상 드라이브의 성능이 저하된 경우에는, 작동성이 **Degraded**로 표시됩니다. 예를 들면 다음과 같습니다.

```
Virtual Drive:
  ID: 0
  Block Size: 512
  Blocks: 3123046400
  Size (MB): 1524925
  Operability: Degraded
  Presence: Equipped
```

**단계 2** RAID 드라이브를 재구축하려면 로컬 디스크 구성 정책 보호를 **no**로 설정합니다. 참고 - 이 단계를 완료하면 디스크의 모든 데이터가 삭제됩니다.

1. 조직 범위를 입력합니다.

**scope org**

2. 로컬 디스크 구성 정책 범위를 입력합니다.

**scope local-disk-config-policy ssp-default**

3. 보호를 **no**로 설정합니다.

**set protect no**

4. 구성을 커밋합니다.

**commit-buffer**

**단계 3** RAID 드라이브가 재구축될 때까지 기다립니다. RAID 재구축 상태를 확인합니다.

**scope chassis 1****show server**

RAID 드라이브가 성공적으로 재구축되면, 슬롯의 전체 상태가 **Ok**로 표시됩니다. 예를 들면 다음과 같습니다.

예제:

```
Server:
  Slot      Overall Status      Service Profile
  -----
  1 Ok      ssp-sprof-1
```

**단계 4** RAID 드라이브가 성공적으로 재구축되면, 로컬 디스크 구성 정책 보호를 다시 **yes**로 설정합니다.



1. 조직 범위를 입력합니다.  
**scope org**
2. 로컬 디스크 컨피그레이션 정책 범위를 입력합니다.  
**scope local-disk-config-policy ssp-default**
3. 보호를 no로 설정합니다.  
**set protect yes**
4. 구성을 커밋합니다.  
**commit-buffer**

## SSD 문제 식별

다음 절차를 사용하여 정보를 수집하고 디바이스에 설치된 SSD에서 발생할 수 있는 문제를 파악합니다. SSD 문제의 한 가지 예시 증상은 DME(Data Management Engine) 프로세스가 시작되지 않는 것입니다.



**참고** 새 SSD를 삽입하면 블레이드 BIOS가 탐지된 후 기본 정보(유형, 모델, SN 등)만 인테리어 아래에 채워집니다. SSP-OS 업그레이드가 완료되어야 인벤토리 아래에 로컬 디스크 데이터가 채워집니다. SSP OS 업그레이드가 여전히 "Updating state(업데이트 중 상태)"인 경우 인벤토리에 로컬 디스크에 대한 항목이 표시되지 않으며 SSD 연결과 관련된 오류 메시지도 표시되지 않습니다.

아래 로깅 파일의 출력에서 SSD에 문제가 있는 경우 TAC에 문의합니다(<https://www.cisco.com/c/en/us/buy/product-returns-replacements-rma.html> 참조).

프로시저

**단계 1** FXOS 명령 셸에 연결합니다.

**connect fxos**

**단계 2** nvram 로깅 파일을 표시합니다.

**show logging nvram**

오류 출력 예:

```
2020 Oct 22 13:03:26 MDCNGIPSAPL02 %$ VDC-1 %$ Oct 22 13:03:25 %KERN-2-SYSTEM_MSG:
[28175880.598580] EXT3-fs error (device sda4): ext3_get_inode_loc: unable to read inode
block - inode=14, block=6
```

**단계 3** 로깅 파일을 표시합니다.

**show logging logfile**

오류 출력 예:

```
2020 Oct 21 21:11:25 (none) kernel: [28118744.718445] EXT3-fs error (device sda4):  
ext3_get_inode_loc: unable to read inode block - inode=14, block=6
```

---

## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.