Firepower 4100/9300 클러스터링

클러스터링을 사용하면 여러 개의 FTD 노드를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. 클러스터링으로 지원되지 않는 기능, 50 페이지의 내용을 참조하십시오.

Firepower 4100/9300 섀시 클러스터링 정보

Firepower 4100/9300 섀시에서 클러스터를 구축할 때는 다음 작업이 수행됩니다.

- 네이티브 인스턴스 클러스터링의 경우: 유닛 간 통신에 사용되는 클러스터 제어 링크(기본값: port-channel 48)를 생성합니다.

  다중 인스턴스 클러스터링의 경우에는 하나 이상의 클러스터 유형 Etherchannel에서 하위 인터페이스를 사전 구성해야 합니다. 각 인스턴스에는 자체 클러스터 제어 링크가 필요 합니다.

  섀시 내 클러스터링(Firepower 9300 전용)의 경우, 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다.

섀시 간 클러스터링의 경우, 섀시 간의 통신을 위해 물리적 인터페이스를 이 EtherChannel에 수동으로 할당해야 합니다.

- 애플리케이션 내부에 클러스터 부트스트랩 구성을 생성합니다.

  클러스터를 구축할 때, 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다.

- 데이터 인터페이스를 *Spanned* 인터페이스로 클러스터에 할당합니다.

  섀시 내 클러스터링의 경우, 스팬 인터페이스는 섀시 간 클러스터링과 마찬가지로 EtherChannel에 국한되지 않습니다. Firepower 9300 수퍼바이저는 EtherChannel 기술을 내부에 사용하여 트래픽을 공유 인터페이스의 다중 모듈에 로드 밸런싱하므로 모든 데이터 인터페이스 유형이 Spanned(스팬) 모드에서 작동합니다. 섀시 간 클러스터링의 경우, 모든 데이터 인터페이스에 Spanned EtherChannel을 사용해야 합니다.

참고 개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

- 관리 인터페이스를 클러스터의 모든 유닛에 할당합니다.

부트스트랩 컨피그레이션

클러스터를 구축할 때, Firepower 4100/9300 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다.

클러스터 멤버

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다.

클러스터의 멤버 중 하나는 제어 유닛입니다. 제어 유닛은 자동으로 결정됩니다. 다른 모든 멤버는 데이터 유닛입니다.

모든 설정은 제어 유닛에서만 수행되어야 하며, 이후 설정이 데이터 유닛에 복제됩니다.

일부 기능은 클러스터로 확장되지 않으며, 제어 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다. 를 참고하십시오.

클러스터 제어 링크

네이티브 인스턴스 클러스터링의 경우: 클러스터 제어 링크는 Port-channel 48 인터페이스를 사용하여 자동으로 생성됩니다.

다중 인스턴스 클러스터링의 경우에는 하나 이상의 클러스터 유형 Etherchannel에서 하위 인터페이스를 사전 구성해야 합니다. 각 인스턴스에는 자체 클러스터 제어 링크가 필요 합니다.

섀시 내 클러스터링의 경우, 이 인터페이스에는 멤버 인터페이스가 없습니다. 이 클러스터 유형 EtherChannel은 인트라 섀시 클러스터링(intra-chassis clustering)을 위한 클러스터 통신에 Firepower

9300 백플레인을 활용합니다. 섀시 간 클러스터링의 경우에는 EtherChannel에 인터페이스를 하나 이상 추가해야 합니다.

2-멤버 섀시 간 클러스터의 경우 클러스터 제어 링크를 한 섀시에서 다른 섀시로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

섀시 간 클러스터링을 위한 클러스터 제어 링크 크기 조정

가능한 경우, 각 섀시의 예상 처리량에 맞게 클러스터 제어 링크의 크기를 조정하여 클러스터 제어 링크가 최악의 시나리오를 처리할 수 있게 해야 합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예를 들면 다음과 같습니다.

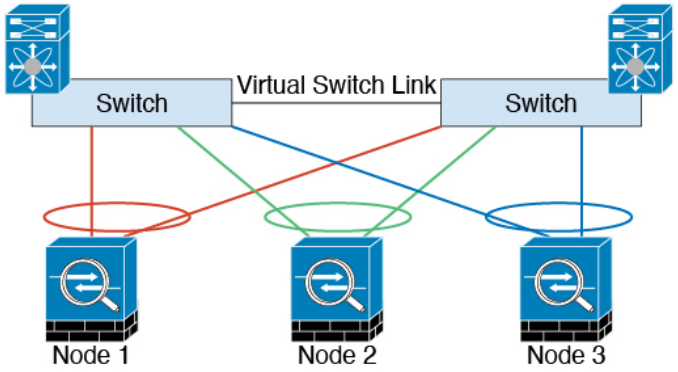
- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

섀시 간 클러스터링을 위한 클러스터 제어 링크 이중화

다음 다이어그램에는 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel) 환경에서 EtherChannel을 클러스터 제어 링크로 사용하는 방법이 나와 있습니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 VSS 또는 vPC의 일부일 경우 방화벽 인터페이스를 동일한 EtherChannel 내에서 연결하여 VSS 또는 vPC의 스위치와 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스팬 EtherChannel입니다.



섀시 간 클러스터링을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(round-trip time)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

클러스터 제어 링크 네트워크

Firepower 4100/9300 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 일반적으로 같은 EtherChannel의 다른 VLAN 하위 인터페이스를 사용하는 다중 인스턴스 클러스터의 경우 VLAN 분리로 인해 서로 다른 클러스터에 같은 IP 주소를 사용할 수 있습니다. 클러스터 제어 링크 네트워크는 유닛 간에 라우터를 포함할 수 없으며 레이어 2 스위칭만 허용됩니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결할 것을 권장합니다. 이 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

클러스터에 관리 유형 인터페이스를 할당해야 합니다. 이 인터페이스는 Spanned 인터페이스와는 다른 특수 개별 인터페이스입니다. 관리 인터페이스를 사용하면 각 유닛에 직접 연결할 수 있습니다. 논리적 관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 Firepower Management Center에 설치하고 등록하는 데 사용됩니다. 또한 자체 로컬 인증, IP 주소 및 정적 라우팅을 사용합니다. 각 클러스터 멤버는 부트스트랩 설정의 일부로 설정하는 관리 네트워크에 별도 IP 주소를 사용합니다.

관리 인터페이스는 논리적 관리 인터페이스와 논리적 진단 인터페이스 간에 공유됩니다. 논리적 진단 인터페이스는 선택 사항이며 부트스트랩 설정의 일부로 구성되어 있지 않습니다. 진단 인터페이스는 다른 데이터 인터페이스와 함께 구성할 수 있습니다. 진단 인터페이스를 설정하기로 선택하면 기본 클러스터 IP 주소를 현재 제어 유닛에 항상 속해 있는 클러스터의 고정 주소로 설정할 수 있습니

다. 주소의 범위를 설정하여 현재 제어 유닛을 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소는 하나의 주소에 지속적인 진단 액세스를 제공합니다. 제어 유닛이 변경되면 기본 클러스터 IP 주소는 새 제어 유닛으로 이동하므로 클러스터에 지속적으로 원활하게 액세스할 수 있습니다. TFTP 또는 시스템 로그 같은 아웃바운드 관리 트래픽의 경우, 제어 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

클러스터 인터페이스

인트라 섀시 클러스터링의 경우, 클러스터에 물리적 인터페이스 또는 Etherchannel(포트 채널)을 할당할 수 있습니다. 클러스터에 할당된 인터페이스는 클러스터의 모든 멤버에 대해 트래픽의 로드 밸런싱을 수행하는 Spanned 인터페이스입니다.

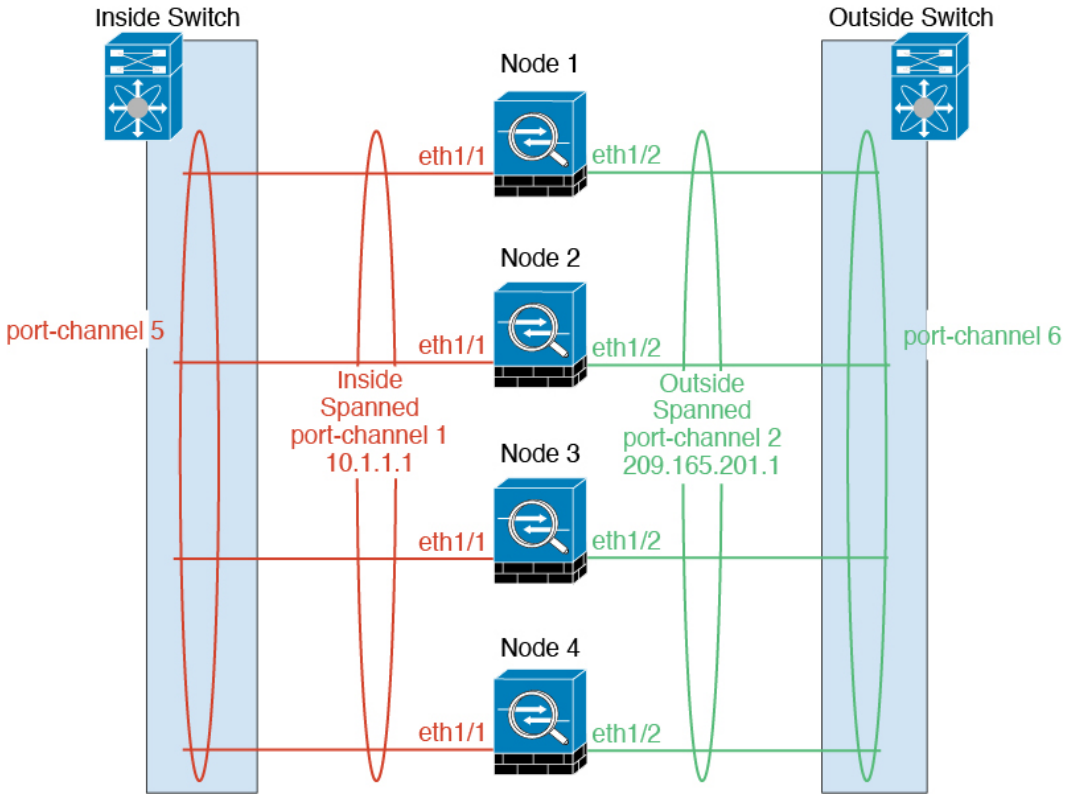
섀시 간 클러스터링의 경우 클러스터에 데이터 Etherchannel만 할당할 수 있습니다. Spanned EtherChannel은 각 섀시에 동일한 멤버 인터페이스를 포함합니다. 업스트림 스위치에서 모든 인터페이스는 단일 EtherChannel에 포함되므로 스위치는 인터페이스가 여러 디바이스와 연결되었는지 알지 못합니다.

개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

스팬 **EtherChannels**

섀시당 하나 이상의 인터페이스를 클러스터 내의 모든 섀시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 스팬 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스가 아닌 BVI에 IP 주소가 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.

다중 인스턴스 클러스터의 경우 각 클러스터에 전용 데이터 EtherChannel이 필요하며 공유 인터페이스 또는 VLAN 하위 인터페이스를 사용할 수 없습니다.



VSS 또는 vPC에 연결

인터페이스에 이중화를 제공하기 위해 Etherchannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.

구성 복제

클러스터의 모든 노드에서는 단일 구성을 공유합니다. 제어 노드에서는 구성만 변경할 수 있으며(부트스트랩 구성 예외), 변경 사항은 클러스터의 모든 다른 노드에 자동으로 동기화됩니다.

클러스터링용 라이선스

개별 노드가 아니라 전체 피처 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 노드는 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

FMC에 클러스터 노드를 추가하는 경우 클러스터에 사용하려는 기능 라이선스를 지정할 수 있습니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **License(**라이선스**)** 영역에서 클러스터에 대한 라이선스를 수정할 수 있습니다.

참고 FMC이 라이선스 되기 전에 (평가 모드에서 실행 되기 전에) 클러스터를 추가하는 경우, FMC를 라이선스하면 클러스터에 정책 변경을 구축할 때 트래픽 중단이 발생할 수 있습니다. 라이선스 모드를 변경하면 모든 데이터 유닛이 클러스터를 벗어났다가 다시 참가합니다.

클러스터링의 요구 사항 및 사전 요구 사항

클러스터 모델 지원

FTD은 다음 모델에서 클러스터링을 지원합니다.

- Firepower 9300 - 클러스터는 유닛을 6개까지 포함할 수 있습니다. 예를 들어 섀시 6개에 모듈 1개, 섀시 3개에 모듈 2개, 또는 모듈을 6개까지 제공하는 어떤 조합도 사용할 수 있습니다. 섀시 내 및 섀시 간 클러스터링 지원
- Firepower 4100- 섀시 간 클러스터링에 최대 유닛 6개 사용 지원

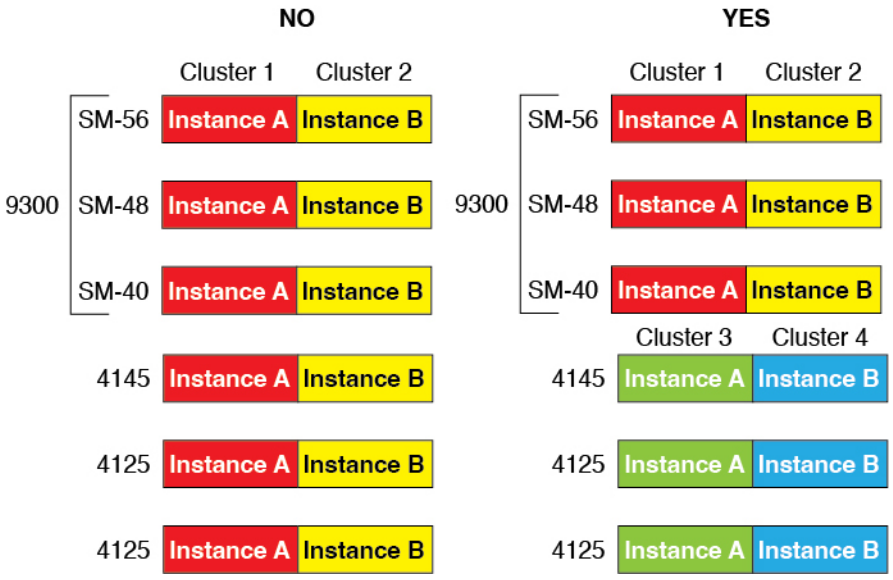
사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

섀시 간 클러스터링 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 섀시:

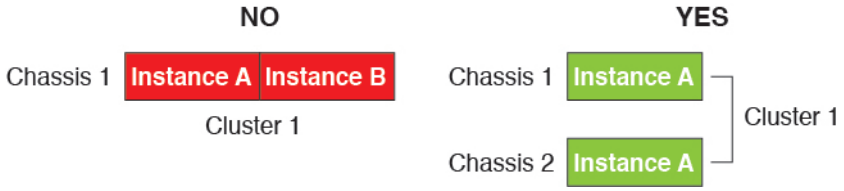
- 네이티브 인스턴스 클러스터링 - Firepower 4100의 경우 모든 섀시가 동일한 모델이어야 합니다. Firepower 9300의 경우: 모든 보안 모듈이 동일한 유형이어야 합니다. 예를 들어 클러스터링을 사용하는 경우 Firepower 9300의 모든 모듈은 SM-40이어야 합니다. 빈 슬롯을 포함하여 섀시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 섀시에 설치된 보안 모듈의 수는 다를 수 있습니다.
- 컨테이너 인스턴스 클러스터링 - 각 클러스터 인스턴스에 동일한 보안 모듈 또는 섀시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 예를 들어 Firepower 9300 SM-56, SM-40, SM-36에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 또는 Firepower 4140 및 4150에서 클러스터를 생성할 수 있습니다.



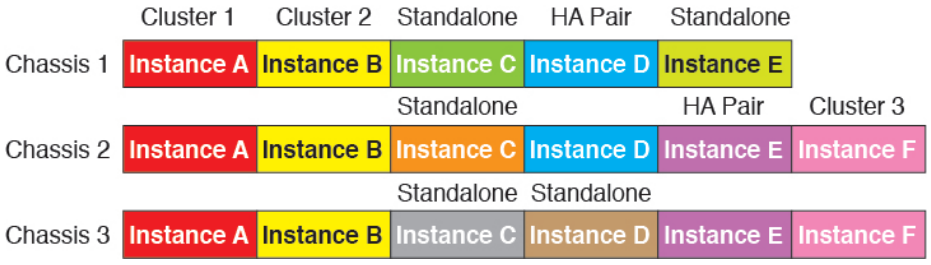
- 이미지 업그레이드 시 동일한 FXOS 소프트웨어 예외를 실행해야 합니다.
- 클러스터에 할당하는 인터페이스에 대한 것과 동일한 인터페이스 구성을 포함해야 합니다(예: EtherChannel, 활성 인터페이스, 속도 및 이중 등). 동일한 인터페이스 ID에 대해 용량이 일치하고 동일한 Spanned EtherChannel에서 성공적인 인터넷 번들링이 가능한 한 섀시에서 서로 다른 네트워크 모듈 유형을 사용할 수 있습니다. 모든 데이터 인터페이스는 섀시 간 클러스터링에서 EtherChannel이어야 합니다. 인터페이스 모듈을 추가 또는 제거하거나 EtherChannel을 구성하는 등의 방법을 통해 클러스터링을 활성화한 후 FXOS에서 인터페이스를 변경하는 경우에는 각 섀시에서 데이터 노드부터 시작하여 마지막으로 제어 노드까지 같은 변경을 수행합니다.
- 동일한 NTP 서버를 사용해야 합니다. FTD의 경우 FMC는 동일한 NTP 서버를 사용해야 합니다. 시간을 수동으로 설정해서는 안 됩니다.

멀티 인스턴스 클러스터링 요구 사항

- 모든 내부 보안 모듈/엔진 클러스터링 안 함 - 지정된 클러스터에 대해 보안 모듈/엔진당 단일 컨테이너 인스턴스만 사용할 수 있습니다. 동일한 모듈에서 실행 중인 경우에는 두 컨테이너 인스턴스를 동일한 클러스터에 추가할 수 없습니다.



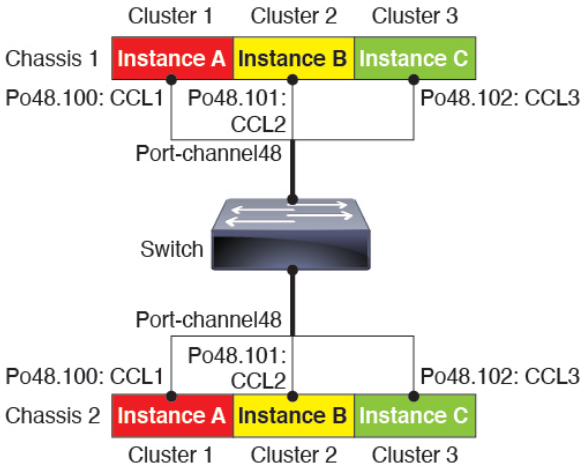
- 클러스터 및 독립형 인스턴스를 혼용 - 보안 모듈/엔진의 모든 컨테이너 인스턴스가 하나의 클러스터에 속할 필요가 없습니다. 일부 인스턴스는 독립형이나 고가용성 노드로 사용할 수 있습니다. 동일한 보안 모듈/엔진에서 별도의 인스턴스를 사용해 여러 클러스터를 생성할 수도 있습니다.



- Firepower 9300의 모든 모듈 세 가지는 해당 클러스터에 속해야 합니다 - Firepower 9300의 경우 클러스터에는 모든 3개의 모듈에서 단일 컨테이너 인스턴스가 필요합니다. 모듈 1 및 2의 인스턴스를 사용하여 클러스터를 생성한 다음 모듈 3 또는 예제에서 네이티브 인스턴스를 사용할 수 없습니다.

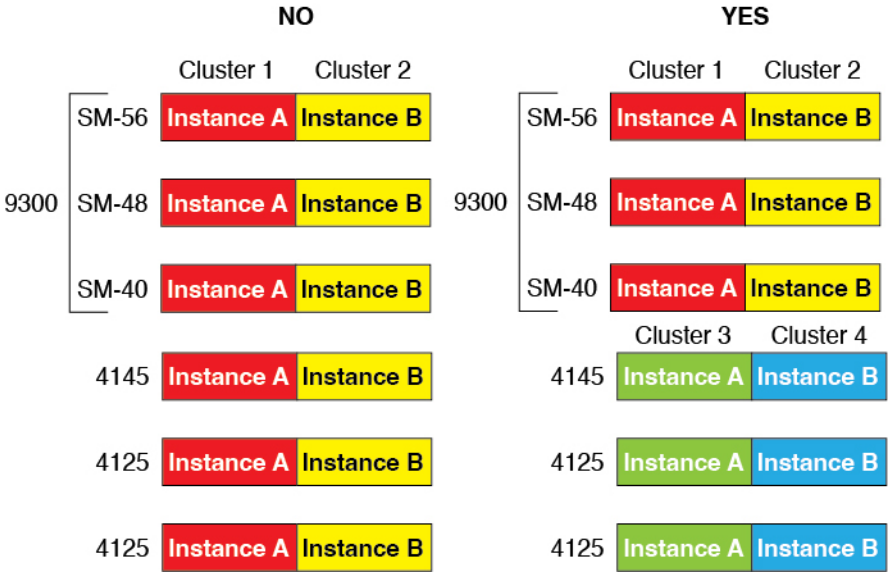
- 리소스 프로파일 일치 - 클러스터의 각 노드가 동일한 리소스 프로파일 특성을 사용하는 것이 좋습니다. 그러나 클러스터 노드를 다른 리소스 프로파일로 변경하거나 다른 모델을 사용하는 경우 일치하지 않는 리소스가 허용됩니다.

- 전용 클러스터 제어 링크 - 섀시 간 클러스터링의 경우 각 클러스터에 전용 클러스터 제어 링크가 필요합니다. 예를 들어 각 클러스터는 동일한 클러스터 유형 EtherChannel에서 별도의 하위 인터페이스를 사용하거나 별도의 EtherChannel을 사용할 수 있습니다.



- 공유 인터페이스 없음 - 클러스터링에서 공유 유형 인터페이스를 지원하지 않습니다. 그러나 동일한 관리 및 이벤트 인터페이스는 여러 클러스터에서 사용할 수 있습니다.

- 하위 인터페이스 없음 - 다중 인스턴스 클러스터는 FXOS 정의 VLAN 하위 인터페이스를 사용할 수 없습니다. 클러스터 EtherChannel의 하위 인터페이스를 사용할 수 있는 클러스터 제어 링크는 예외입니다.
- 섀시 모델 혼합 - 각 클러스터 인스턴스에 동일한 보안 모듈 또는 섀시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 예를 들어 Firepower 9300 SM-56, SM-40, SM-36에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 또는 Firepower 4140 및 4150에서 클러스터를 생성할 수 있습니다.



- 최대 6개 노드 - 하나의 클러스터에서 최대 6개의 컨테이너 인스턴스를 사용할 수 있습니다.

섀시 간 클러스터링을 위한 스위치 요구 사항

- Firepower 4100/9300 섀시에서 클러스터링을 구성하기 전에 스위치 구성을 완료하고 섀시의 모든 EtherChannel을 스위치에 성공적으로 연결하십시오.
- 지원되는 스위치 특성은 Cisco FXOS 호환성을 참고하십시오.

클러스터링 지침 및 제한 사항

섀시 간 클러스터링을 위한 스위치

- 연결된 스위치가 클러스터 데이터 인터페이스 및 클러스터 제어 링크 인터페이스 모두의 MTU와 일치해야 합니다. 클러스터 제어 링크 인터페이스 MTU를 데이터 인터페이스 MTU보다 100바이트 이상 높게 설정해야 하므로 스위치를 연결하는 클러스터 제어 링크를 적절하게 설정해야 합니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다.

- Cisco IOS XR 시스템의 경우 기본이 아닌 MTU를 설정하려면 IOS 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면, **mtu-ignore** 옵션을 사용하지 않는 경우 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 IOS *IPv4* MTU와 일치해야 합니다. Cisco Catalyst 및 Cisco Nexus 스위치에는 이 조정이 필요하지 않습니다.
- 클러스터 제어 링크 인터페이스용 스위치의 경우, 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 디바이스에 트래픽이 균일하지 않게 분산될 수 있습니다.
- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 비활성화하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 클러스터 제어 링크 경로의 스위치에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다.
- Supervisor 2T EtherChannel에서 기본 해시 분산 알고리즘은 적응형입니다. VSS 설계에서 비대칭 트래픽을 방지하려면 클러스터 디바이스에 연결된 포트 채널의 해시 알고리즘을 다음과 같이 변경하여 수정합니다.

  router(config) # **port-channel** *id* **hash-distribution fixed**

  VSS 피어 링크의 적응형 알고리즘을 활용할 때가 있을 수 있으므로 알고리즘을 전역으로 변경하지 마십시오.

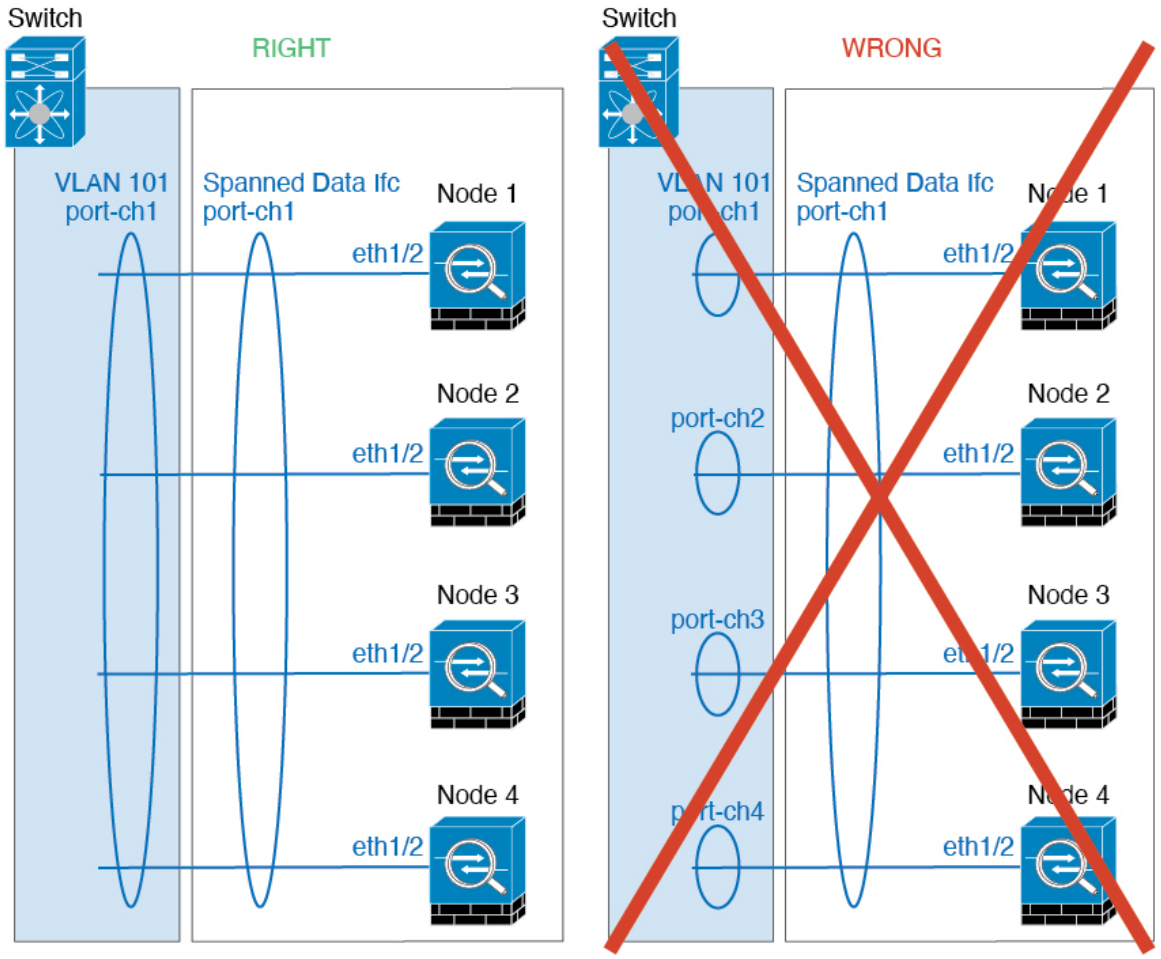
- Firepower 4100/9300 클러스터는 LACP 단계적 통합을 지원합니다. 따라서 연결된 Cisco Nexus 스위치에서 LACP 단계적 통합을 활성화된 상태로 둘 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다. FXOS EtherChannel에서는 기본적으로 LACP 속도가 fast(고속)로 설정됩니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP를 지원하지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.

섀시 간 클러스터링을 위한 **EtherChannel**

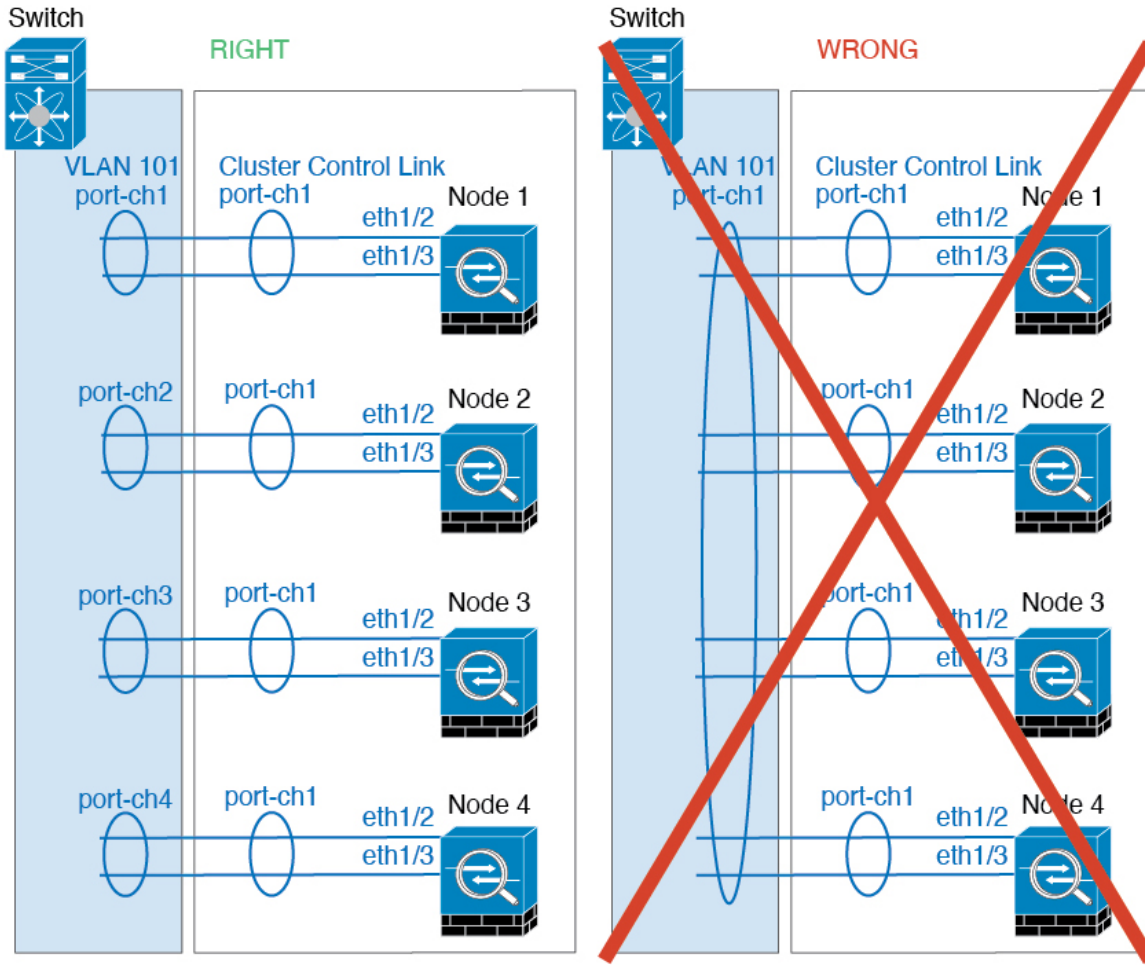
- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel

이 교차 스택에 연결되어 있는 상태에서 제어 유닛 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.

- Spanned EtherChannel 구성과 디바이스-로컬 EtherChannel 구성 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에서 각각 알맞게 스위치를 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 스팬 EtherChannels의 경우, 인터페이스가 스위치의 단일 EtherChannel에 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



  - 디바이스-로컬 EtherChannel - 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 클러스터 유닛 디바이스-로컬 EtherChannel의 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 클러스터 유닛 EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



추가 지침

- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel 인터페이스에 연결된 Windows 2003 서버를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않아 대량의 ICMP 메시지가 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.
- 이중화를 위해 EtherChannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.
- 섀시 내에서 일부 보안 모듈을 클러스터하여 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.

- 암호 해독된 TLS/SSL 연결의 경우, 암호 해독 상태가 동기화되지 않습니다. 연결 소유자 장애가 발생하는 경우, 암호 해독된 연결이 재설정됩니다. 새 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.

기본값

- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 실패한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도하도록 설정됩니다.
- 실패한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도하도록 설정됩니다.
- 5초 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

클러스터링 구성

Firepower 4100/9300 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다. FMC에 유닛을 추가하고 클러스터로 그룹화할 수 있습니다.

FXOS: FTD 클러스터 추가

네이티브 모드에서 단일 Firepower 9300 섀시를 섀시 내 클러스터로 추가하거나 섀시 간 클러스터링용으로 여러 섀시를 추가할 수 있습니다.

다중 인스턴스 모드에서 단일 Firepower 9300 섀시에 하나 이상의 클러스터를 섀시 내 클러스터로 추가하거나(각 모듈에 인스턴스를 포함해야 함) 섀시 간 클러스터링용으로 여러 섀시에 하나 이상의 클러스터를 추가할 수 있습니다.

섀시 간 클러스터링의 경우 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 추가한 다음 쉽게 구축하기 위해 첫 번째 섀시의 부트스트랩 구성을 다음 섀시에 복사합니다.

FTD 클러스터 생성

Firepower 4100/9300 섀시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다.

섀시 간 클러스터링의 경우 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 섀시의 부트스트랩 컨피그레이션을 다음 섀시에 복사합니다.

모듈을 설치하지 않은 경우에도 Firepower 9300 섀시의 3개 모듈 슬롯 모두 또는 컨테이너 인스턴스, 각 슬롯의 컨테이너 인스턴스에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음, 해당 이미지를 Firepower 4100/9300 섀시에 업로드합니다.
- 컨테이너 인스턴스의 경우 기본 프로필을 사용하지 않으려면 컨테이너 인스턴스에 대한 리소스 프로파일 추가에 따라 리소스 프로필을 추가합니다.
- 컨테이너 인스턴스의 경우 컨테이너 인스턴스를 처음으로 설치하기 전에 디스크가 올바른 형식을 갖도록 보안 모듈/엔진을 다시 초기화해야 합니다. **Security Modules(**보안 모듈**)** 또는 **Security Engine(**보안 엔진**)**을 선택하고 다시 초기화 아이콘(🔄)을 클릭합니다. 기존 논리적 디바이스가 삭제된 후에 새 디바이스로 재설치되며 로컬 애플리케이션 구성은 손실됩니다. 기본 인스턴스를 컨테이너 인스턴스로 교체할 때는 어떤 경우든 기본 인스턴스를 삭제해야 합니다. 기본 인스턴스를 컨테이너 인스턴스로 자동 마이그레이션할 수는 없습니다.
- 다음 정보를 수집합니다.
  - 관리 인터페이스 ID, IP 주소, 네트워크 마스크
  - 게이트웨이 IP 주소
  - FMC 선택한 IP 주소 및/또는 NAT ID
  - DNS 서버 IP 주소
  - FTD 호스트 이름 및 도메인 이름

프로시저

단계 **1** 인터페이스를 구성합니다.

a) 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(port-channel이라고도 함)을 최소 1개 추가합니다. EtherChannel(포트 채널) 추가 또는 실제 인터페이스 구성를 참조하십시오.

섀시 간 클러스터링의 경우, 모든 데이터 인터페이스는 멤버 인터페이스가 최소 1개 있는 Spanned EtherChannel이어야 합니다. 각 섀시에 동일한 EtherChannel을 추가합니다. 스위치의 단일 EtherChannel에 모든 클러스터 유닛의 멤버 인터페이스를 결합합니다. 섀시 간 클러스터링을 위한 EtherChannel에 대한 자세한 내용은 클러스터링 지침 및 제한 사항, 10 페이지을 참조하십시오.

다중 인스턴스 클러스터링의 경우 클러스터의 FXOS 정의 VLAN 하위 인터페이스 또는 데이터 공유 인터페이스를 사용할 수 없습니다. 애플리케이션 정의 하위 인터페이스만 지원됩니다. 자세한 내용은 FXOS 인터페이스와 애플리케이션 인터페이스 비교를 참조하십시오.

b) 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. EtherChannel(포트 채널) 추가 또는 실제 인터페이스 구성를 참조하십시오.

관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 인터페이스(FXOS에서 MGMT, management0 또는 기타 유사한 이름으로 표시되는 섀시 관리 인터페이스 확인 가능)와는 다릅니다.

섀시 간 클러스터링의 경우 각 섀시에 동일한 Management(관리) 인터페이스를 추가합니다.

멀티 인스턴스 클러스터링의 경우 동일한 섀시의 여러 클러스터 또는 독립형 인스턴스에서 동일한 관리 인터페이스를 공유할 수 있습니다.

c) 섀시간 클러스터링의 경우, 멤버 인터페이스를 클러스터 제어 링크 EtherChannel에 추가합니다(기본: 포트 채널 48). EtherChannel(포트 채널) 추가의 내용을 참조하십시오.

인트라 섀시 클러스터링(intra-chassis clustering)용으로 멤버 인터페이스를 추가하지 마십시오. 멤버를 추가하면 섀시에서는 이 클러스터를 섀시 간 클러스터로 가정하며, 예를 들어 Spanned EtherChannel만 사용하도록 허용합니다.

멤버 인터페이스가 포함되지 않은 경우, **Interfaces(**인터페이스**)** 탭에서 port-channel 48 클러스터 유형 인터페이스에 **Operation State(**운영 상태**)**가 **failed(**실패**)**로 표시됩니다. 인트라 섀시 클러스터링(intra-chassis clustering)의 경우 이 EtherChannel에는 멤버 인터페이스가 필요하지 않으므로 이 Operation State(운영 상태)를 무시할 수 있습니다.

각 섀시에 동일한 멤버 인터페이스를 추가합니다. 클러스터 제어 링크는 각 섀시의 디바이스-로컬 EtherChannel입니다. 디바이스별 스위치에서 별도의 EtherChannel을 사용합니다. 섀시 간 클러스터링을 위한 EtherChannel에 대한 자세한 내용은 클러스터링 지침 및 제한 사항, 10 페이지을 참조하십시오.

다중 인스턴스 클러스터링의 경우 추가 클러스터 유형 Etherchannel를 생성할 수 있습니다. 관리 인터페이스와 달리 클러스터 제어 링크는 여러 디바이스에서 공유할 수 없으므로 각 클러스터에 대한 클러스터 인터페이스가 필요합니다. 그러나 여러 Etherchannel 대신 VLAN 하위 인터페이스를 사용하는 것이 좋습니다. 클러스터 인터페이스에 VLAN 하위 인터페이스를 추가하려면 다음 단계를 참조하십시오.

d) 다중 인스턴스 클러스터링의 경우 각 클러스터에 별도의 클러스터 제어 링크를 사용할 수 있도록 VLAN 하위 인터페이스를 클러스터 EtherChannel에 추가합니다. 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가의 내용을 참조하십시오.

클러스터 인터페이스에 하위 인터페이스를 추가하면 네이티브 클러스터에서 해당 인터페이스를 사용할 수 없습니다.

e) (선택 사항) 이벤트 인터페이스를 추가합니다. EtherChannel(포트 채널) 추가 또는 실제 인터페이스 구성를 참조하십시오.

이 인터페이스는 FTD 디바이스의 보조 관리 인터페이스입니다. 이 인터페이스를 사용하려면 FTD CLI에서 해당 IP 주소 및 기타 매개변수를 구성해야 합니다. 예를 들면 관리 트래픽을 이벤트(예: 웹 이벤트)에서 분리할 수 있습니다. FTD 명령 참조에서 **configure network** 명령을 참조하십시오.

섀시 간 클러스터링의 경우 각 섀시에 동일한 Eventing 인터페이스를 추가합니다.

단계 **2** **Logical Devices(**논리적 디바이스**)**를 선택합니다.

단계 **3** **Add(**추가**)** > **Cluster(**클러스터**)**를 클릭하고 다음 파라미터를 설정합니다.

그림 *1:* 네이티브 클러스터

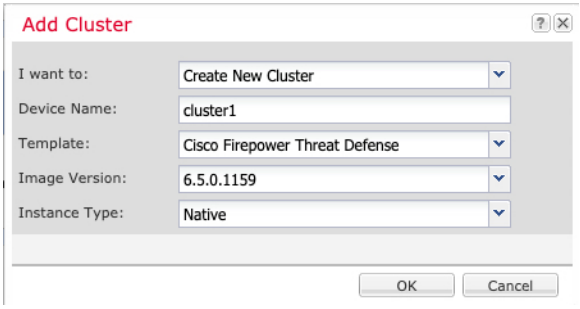
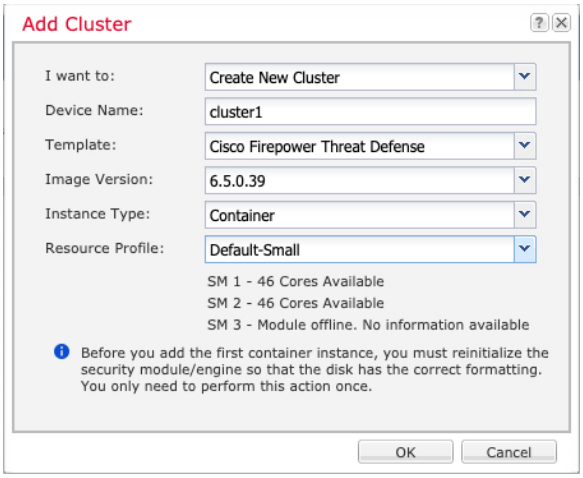


그림 *2:* 다중 인스턴스 클러스터



a) **I want to:(**수행할 작업**:)** > **Create New Cluster(**새 클러스터 생성**)**를 선택합니다.

b) **Device Name(**디바이스 이름**)**을 입력합니다.

이 이름은 내부적으로 섀시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

c) **Template(**템플릿**)**에서 **Cisco Firepower Threat Defense**를 선택합니다.

d) **Image Version(**이미지 버전**)**을 선택합니다.

e) **Instance Type(**인스턴스 유형**)**의 경우 **Native(**네이티브**)** 또는 **Container(**컨테이너**)**를 선택합니다.

네이티브 인스턴스는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다. 컨테이너 인스턴스는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다.

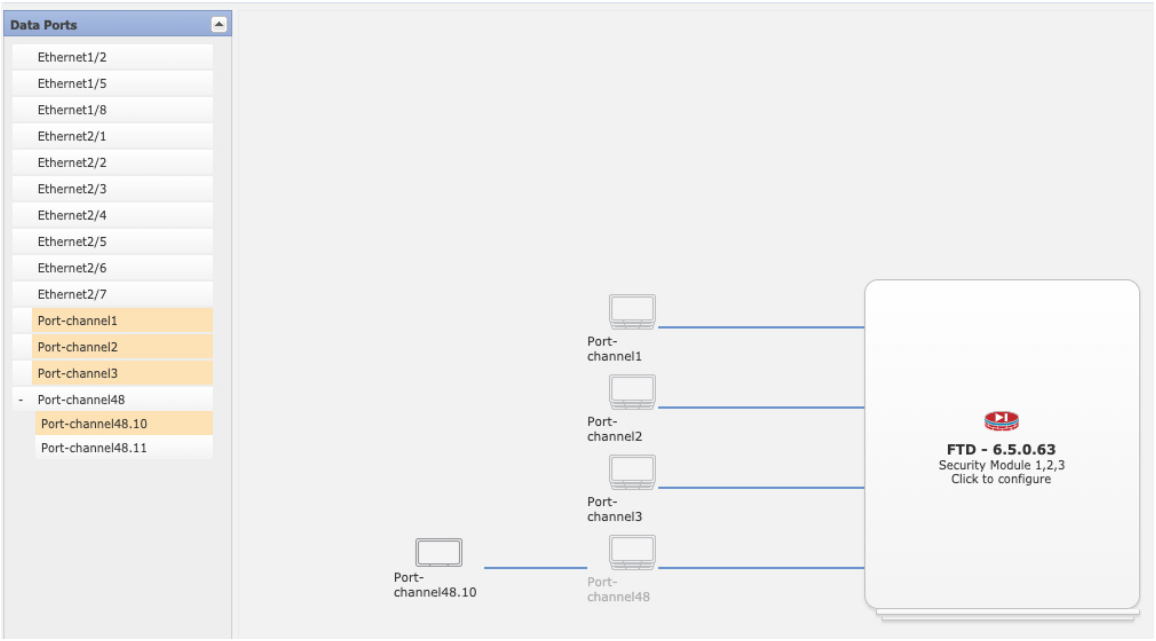
f) (컨테이너 인스턴스만 해당) **Resource Type(**리소스 유형**)**의 드롭다운 목록에서 리소스 프로파일 중 하나를 선택합니다.

Firepower 9300의 경우 이 프로파일은 보안 모듈의 각 인스턴스에 적용됩니다. 이 절차에서 나중에 보안 모듈별로 서로 다른 프로파일을 설정할 수 있습니다. 예를 들어 다른 보안 모듈 유형을 사용하면서 더 성능이 낮은 모델에서 더 많은 CPU를 사용할 수도 있습니다. 클러스터를 생성하기 전에 올바른 프로파일을 선택하는 것이 좋습니다. 새 프로파일을 생성해야 하는 경우 클러스터 생성을 취소하고 컨테이너 인스턴스에 대한 리소스 프로파일 추가을 사용해 하나를 추가합니다.

g) **OK(**확인**)**를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 **4** 이 클러스터에 할당할 인터페이스를 선택합니다.



네이티브 모드 클러스터링의 경우: 유효한 모든 인터페이스가 기본적으로 할당되어 있습니다. 여러 클러스터 유형의 인터페이스를 지정했다면 하나를 제외하고 모두 선택 해제합니다.

다중 인스턴스 클러스터링의 경우: 클러스터에 할당할 각 데이터 인터페이스를 선택하고 클러스터 유형 포트 채널 또는 포트 채널 하위 인터페이스도 선택합니다.

단계 **5** 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 **6** **Cluster Information(**클러스터 정보**)** 페이지에서 다음 작업을 수행합니다.

그림 *3:* 네이티브 클러스터

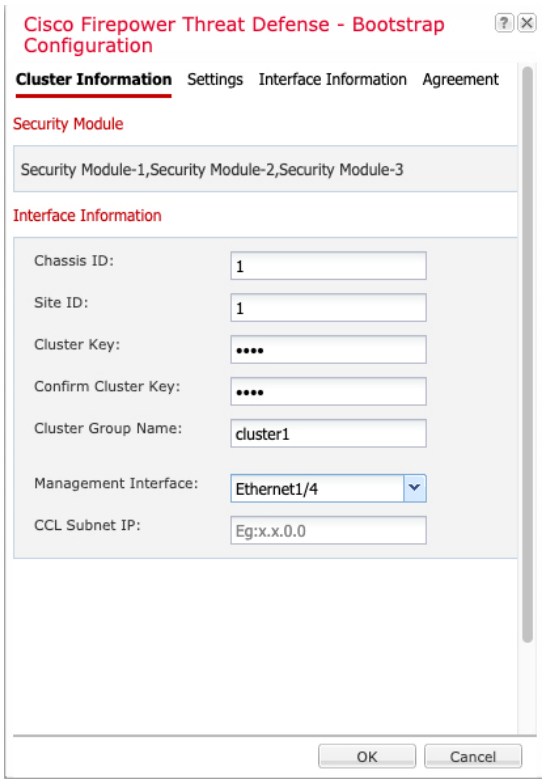
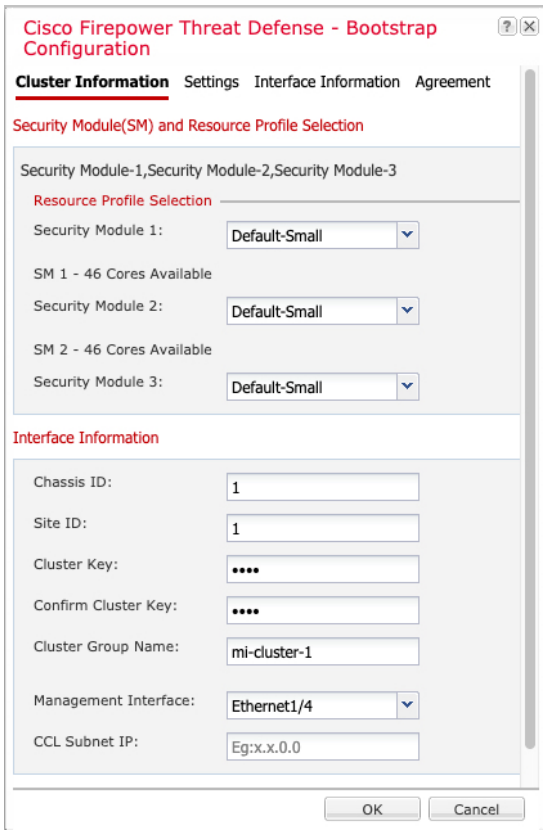


그림 *4:* 다중 인스턴스 클러스터



a) (Firepower 9300 컨테이너 인스턴스만 해당) 보안 모듈**(SM)** 및 리소스 프로파일 선택 영역에서 모듈별로 다른 리소스 프로파일을 설정할 수 있습니다. 예를 들어 다른 보안 모듈 유형을 사용하면서 더 성능이 낮은 모델에서 더 많은 CPU를 사용할 수도 있습니다.

b) 섀시 간 클러스터링의 경우, **Chassis ID(**섀시 **ID)** 필드에 섀시 ID를 입력합니다. 클러스터의 각 섀시는 고유 ID를 사용해야 합니다.

   이 필드는 클러스터 제어 링크 Port-Channel 48에 멤버 인터페이스를 추가한 경우에만 나타납니다.

c) 사이트 간 클러스터링의 경우 이 섀시에 대해 **Site ID(**사이트 **ID)** 필드에 1~8의 사이트 ID를 입력합니다. FlexConfig 기능. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 FMC FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.

d) **Cluster Key(**클러스터 키**)** 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다.

   공유 비밀은 1자 ~ 63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 옵션은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

e) **Cluster Group Name(**클러스터 그룹 이름**)**(논리적 디바이스 구성의 클러스터 그룹 이름)을 설정합니다.

이름은 1자 ~ 38자로 된 ASCII 문자열이어야 합니다.

f) **Management Interface(**관리 인터페이스**)**를 선택합니다.

이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 섀시 관리 포트와 별개입니다.

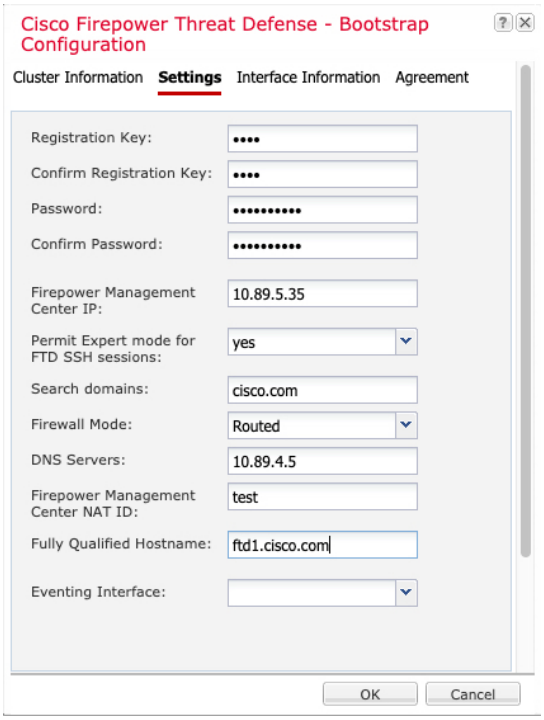
하드웨어 바이패스 지원 인터페이스를 Management(관리) 인터페이스로 할당할 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다.

g) (선택 사항) **CCL Subnet IP(CCL** 서브넷 **IP)**를 *a.b***.0.0**으로 설정합니다.

기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 이 경우 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 및 내부 (169.254.0.0/16) 주소를 제외한 모든 /16 네트워크 주소를 클러스터용 고유 네트워크에 지정합니다. 값을 0.0.0.0으로 설정하는 경우 기본 네트워크가 사용됩니다.

섀시에서는 섀시 ID 및 슬롯 ID *a.b.chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.

단계 **7** **Settings(**설정**)** 페이지에서 다음 작업을 완료합니다.



a) **Registration Key(**등록 키**)**필드에 등록하는 동안 FMC와 클러스터 멤버 간에 공유할 키를 입력합니다.

이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.

b) FTD 관리 사용자가 CLI에 액세스할 때 사용할 **Password(**비밀번호**)**를 입력합니다.

c) **Firepower Management Center IP** 필드에 FMC를 관리하기 위한 IP 주소를 입력합니다. FMC IP 주소를 알 수 없는 경우, 이 필드를 비워두고 **Firepower Management Center NAT ID** 필드에 암호를 입력합니다.

d) (선택 사항) 컨테이너 인스턴스의 경우, **Permit Export mode from FTD SSH sessions(FTD SSH** 세션에서 전문가 모드 허용**)**에 대해 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다. 전문가 모드에서는 고급 트러블슈팅을 위한 FTD 셸 액세스 기능이 제공됩니다.

이 옵션에 대해 **Yes(**예**)**를 선택하는 경우 SSH 세션에서 컨테이너 인스턴스에 직접 액세스할 수 있는 사용자가 전문가 모드를 시작할 수 있습니다. **No(**아니요**)**를 선택하는 경우에는 FXOS CLI에서 컨테이너 인스턴스에 액세스할 수 있는 사용자만 전문가 모드를 시작할 수 있습니다. 각 인스턴스를 더욱 명확하게 격리할 수 있도록 **No(**아니요**)**를 선택하는 것이 좋습니다.

문서에 설명되어 있는 절차에 따라 Expert 모드가 필요하다고 알려주는 경우 또는 Cisco Technical Assistance Center에서 사용하도록 요청하는 경우에만 Expert 모드를 사용합니다. 이 모드를 설정하려면 FTD CLI에서 **expert** 명령을 사용합니다.

e) (선택 사항) **Search Domains(**검색 도메인**)** 필드에 관리 네트워크의 쉼표로 구분된 검색 도메인 목록을 입력합니다.

f) (선택 사항) **Firewall Mode(**방화벽 모드**)** 드롭다운 목록에서 **Transparent(**투명**)** 또는 **Routed(**라우팅됨**)**를 선택합니다.

라우팅 모드에서 FTD는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

g) (선택 사항) **DNS Servers(DNS** 서버**)** 필드에 쉼표로 구분된 DNS 서버 목록을 입력합니다.

예를 들어, FMC의 호스트 이름을 지정하는 경우, FTD에서는 DNS를 사용합니다.

h) (선택 사항) 새 디바이스로 클러스터를 추가할 때 FMC에도 입력할 암호를 **Firepower Management Center NAT ID** 필드에 입력합니다.

일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. 1~37자의 임의의 텍스트 문자열을 NAT ID로 지정할 수 있습니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

i) (선택 사항) **Fully Qualified Hostname(**정규화된 호스트 이름**)** 필드에 FTD 디바이스의 정규화된 이름을 입력합니다.

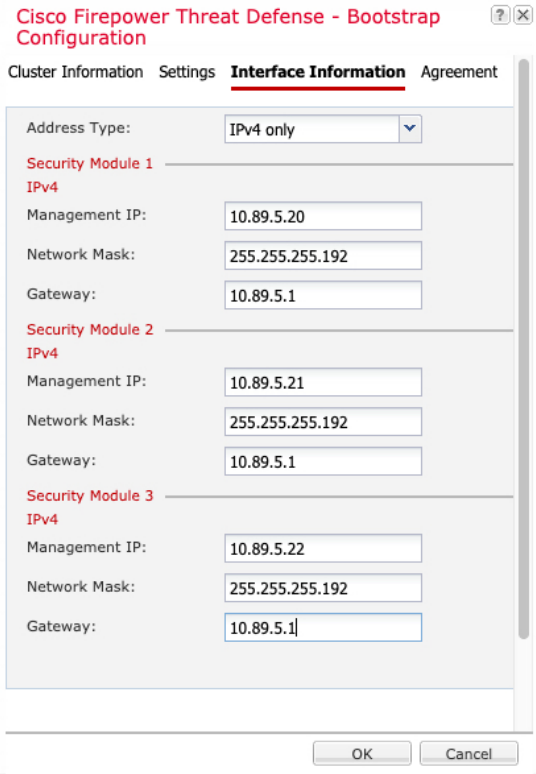
유효한 문자는 a부터 z까지의 문자, 0과 9 사이의 숫자, 점(.) 및 하이픈(-)입니다. 최대 문자 수는 253자입니다.

j) (선택 사항) **Eventing Interface(Eventing** 인터페이스**)** 드롭다운 목록에서 이벤트가 전송되어야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

이벤트에 사용할 별도의 인터페이스를 지정하려면 인터페이스를 *Firepower* 이벤트 처리 인터페이스로 구성해야 합니다. 하드웨어 바이패스 지원 인터페이스를 Eventing(이벤트) 인터페이스로 할당하는 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다.

단계 **8** **Interface Information(**인터페이스 정보**)** 페이지에서 클러스터의 각 보안 모듈의 관리 IP 주소를 구성합니다. **Address Type(**주소 유형**)** 드롭다운 목록에서 주소 유형을 선택한 다음 각 보안 모듈에 대해 다음 작업을 수행합니다.

참고 모듈을 설치하지 않은 경우에도 섀시의 3개 모듈 슬롯 모두에 대해 IP 주소를 설정해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.



a) **Management IP(**관리 **IP)** 필드에서 IP 주소를 구성합니다.

각 모듈에 대해 동일한 네트워크에서 고유한 IP 주소를 지정합니다.

b) **Network Mask(**네트워크 마스크**)** 또는 **Prefix Length(**접두사 길이**)**를 입력합니다.

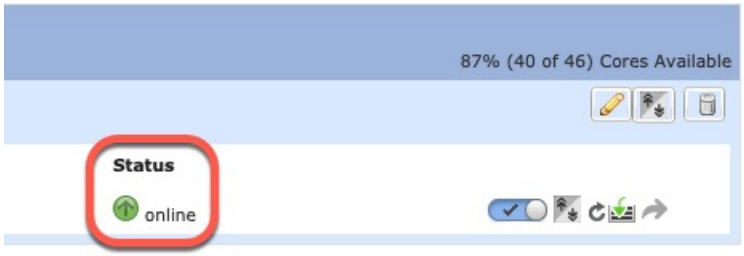
c) **Network Gateway(**네트워크 게이트웨이**)** 주소를 입력합니다.

단계 **9** **Agreement(**계약**)** 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 **10** **OK(**확인**)**를 클릭하여 구성 대화 상자를 닫습니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 상태가 **online(**온라인**)**으로 표시되면 나머지 클러스터 섀시를 추가할 수도 있고, 섀시 내 클러스터링의 경우 애플리케이션 내에서 클러스터 구성을 시작할 수도 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 **12** 섀시 간 클러스터링의 경우, 다음 섀시를 클러스터에 추가합니다.

a) Firepower Chassis Manager의 첫 번째 섀시에서 오른쪽 상단에 있는 **Show Configuration(**구성 표시**)** 아이콘을 클릭하여 표시된 클러스터 구성을 복사합니다.

b) 다음 섀시에 있는 Firepower Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.

c) **I want to:(**수행할 작업**:) > Join an Existing Cluster(**기존 클러스터에 조인**)**를 선택합니다.

d) **OK(**확인**)**를 클릭합니다.

e) **Copy Cluster Details(**클러스터 세부사항 복사**)** 상자에서 첫 번째 섀시의 클러스터 구성에 붙여 넣고 **OK(**확인**)**를 클릭합니다.

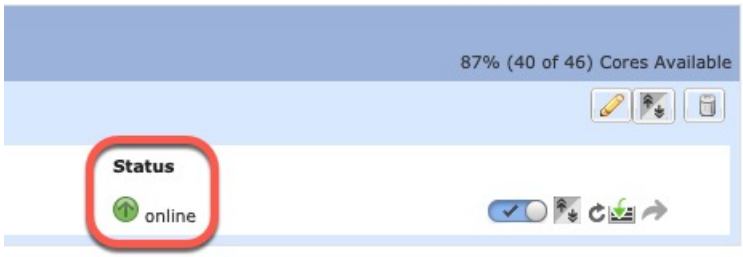
f) 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID(**섀시 **ID) -** 고유한 섀시 ID를 입력합니다.
- **Site ID(**사이트 **ID) -** 사이트 간 클러스터링의 경우 이 섀시에 대해 1~8 사이의 사이트 ID를 입력합니다. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 FMC FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.
- **Cluster Key(**클러스터 키**) -** (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP(**관리 **IP) -** 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유 IP 주소로 변경합니다.

OK(확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 **13** 관리 IP 주소를 사용하여 제어 유닛을 FMC에 추가합니다.

FMC에 추가하기 전에 모든 클러스터 유닛이 FXOS에서 성공적으로 형성된 클러스터에 있어야 합니다.

그러면 FMC에서 데이터 유닛을 자동으로 탐지합니다.

클러스터 노드 추가

기존 클러스터에서 FTD 클러스터 노드를 추가하거나 교체합니다.FXOS에서 새 클러스터 노드를 추가할 때 FMC에서는 노드를 자동으로 추가합니다.

참고 이 절차의 FXOS 단계는 새 섀시 추가 시에만 적용됩니다. 클러스터링이 이미 활성화된 Firepower 9300에 새 모듈을 추가하는 경우에는 모듈이 자동으로 추가됩니다.

시작하기 전에

- 교체 시 기존 클러스터 노드를 FMC에서 삭제해야 합니다. 새 노드로 교체할 경우, 해당 유닛은 FMC에서 새 디바이스로 간주됩니다.

- 인터페이스 구성은 새 섀시에서 동일해야 합니다. FXOS 섀시 구성 내보내기와 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.

프로시저

단계 **1** 이전에 FMC를 사용하여 FTD 이미지를 업그레이드한 경우 클러스터의 각 섀시에서 다음 단계를 수행합니다.

FMC에서 업그레이드할 때 FXOS 구성의 시작 버전이 업데이트되지 않았으며 독립형 패키지가 섀시에 설치되지 않았습니다. 새 노드가 올바른 이미지 버전을 사용하여 클러스터에 참여할 수 있도록 이러한 항목을 모두 수동으로 설정해야 합니다.

참고 패치 릴리스만 적용한 경우 이 단계를 건너뛸 수 있습니다. Cisco는 패치용 독립형 패키지를 제공하지 않습니다.

a) **System(**시스템**)** > **Updates(**업데이트**)** 페이지를 사용하여 섀시에 실행 중인 FTD 이미지를 설치합니다.

b) **Logical Devices(**논리적 디바이스**)**를 클릭하고 버전 설정 아이콘( )를 클릭합니다. 여러 모듈이 있는 Firepower 9300의 경우 각 모듈의 버전을 설정합니다.

Startup Version(시작 버전**)**에는 구축에 사용한 원래 패키지가 표시됩니다. **Current Version(**현재 버전**)**에는 업그레이드한 버전이 표시됩니다.

c) **New Version(**새 버전**)** 드롭다운 메뉴에서 업로드한 버전을 선택합니다. 이 버전은 표시된 현재 버전과 일치해야 하며, 새 버전과 일치하도록 시작 버전을 설정합니다.

d) 새 섀시에 새 이미지 패키지가 설치되어 있는지 확인합니다.

단계 **2** 기존 클러스터 섀시 Firepower Chassis Manager에서 **Logical Devices(**논리적 디바이스**)**를 클릭합니다.

단계 **3** 오른쪽 상단에 있는 설정 표시 아이콘을 클릭하여 표시된 클러스터 설정을 복사합니다.

단계 **4** 새 섀시에서 Firepower Chassis Manager에 연결한 다음 **Add(**추가**)** > **Cluster(**클러스터**)**를 클릭합니다.

단계 **5** **Device Name(**디바이스 이름**)**에 논리적 디바이스의 이름을 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Copy Cluster Details(**클러스터 세부사항 복사**)** 상자에서 첫 번째 섀시의 클러스터 구성에 붙여 넣고 **OK(**확인**)**를 클릭합니다.

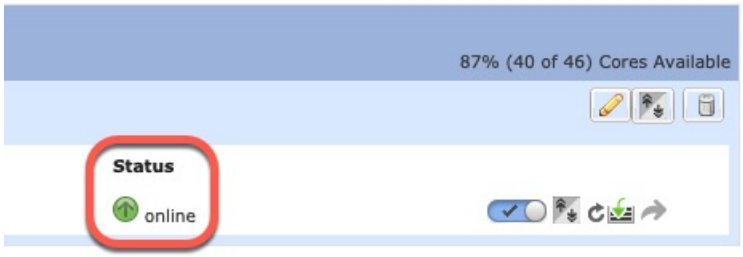
단계 **8** 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID(**섀시 **ID)** - 고유한 섀시 ID를 입력합니다.
- **Site ID(**사이트 **ID)** - 사이트 간 클러스터링의 경우 이 섀시에 대해 1~8 사이의 사이트 ID를 입력합니다. FMC FlexConfig 기능을 통해서만 이 기능을 구성할 수 있습니다.
- **Cluster Key(**클러스터 키**)** - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP(**관리 **IP)** - 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유 IP 주소로 변경합니다.

OK(확인**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



FMC: 클러스터 추가

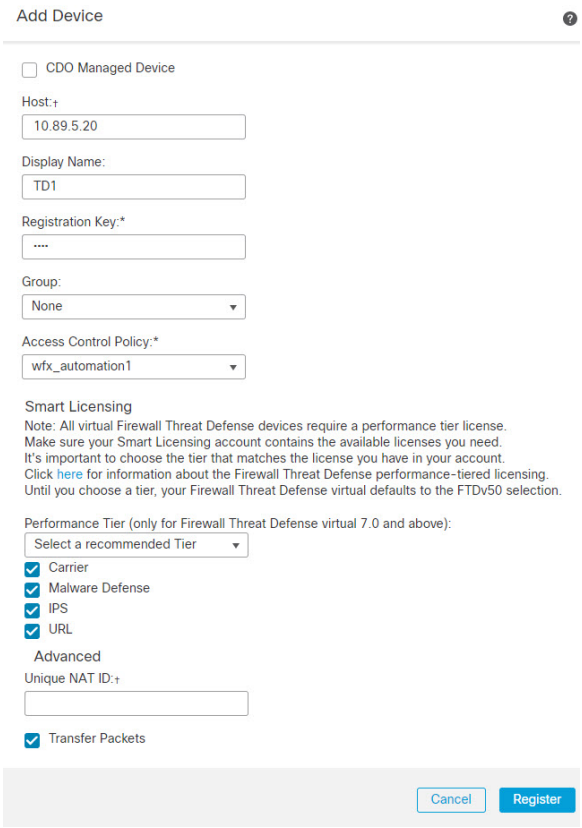
Firepower Management Center에 클러스터 유닛 중 하나를 새 장치로 추가합니다. FMC는 다른 클러스터 멤버를 자동으로 감지합니다.

시작하기 전에

- 클러스터를 추가하기 위한 이 방법은 FTD 버전 6.2 이상이 필요합니다. 이전 버전 디바이스를 관리해야 하는 경우 해당 버전의 Firepower Management Center 환경 설정 가이드를 참조합니다.
- FMC에 추가하기 전에 모든 클러스터 유닛이 FXOS에서 성공적으로 형성된 클러스터에 있어야 합니다. 제어 유닛을 확인하십시오. Firepower Chassis Manager **Logical Devices(**논리적 디바이스**)** 화면을 참조하거나 FTD **show cluster info** 명령을 사용합니다.

프로시저

단계 **1** FMC에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 클러스터 구축 시 할당한 유닛의 관리 IP 주소를 사용해 제어 유닛을 추가하기 위해 **Add(**추가**)** > **Add Device(**디바이스 추가**)**를 선택합니다.



a) **Host(**호스트**)** 필드에 제어 유닛의 IP 주소나 호스트 이름을 입력합니다.

   최적의 성능을 위해서는 제어 유닛을 추가하는 것이 좋습니다 하지만 모든 클러스터 유닛을 추가할 수 있습니다.

   디바이스 설정 중에 NAT ID를 사용한 경우 이 필드를 입력하지 않아도 됩니다.자세한 내용은 NAT 환경를 참조하십시오.

b) FMC에 표시할 제어 유닛의 이름을 표시 이름 필드에 입력합니다.

   이 표시 이름은 클러스터용이 아닙니다. 추가하려는 제어 유닛에만 해당됩니다. 나중에 다른 클러스터 멤버의 이름과 클러스터 표시 이름을 변경할 수 있습니다.

c) FXOS에 클러스터를 구축할 때 사용한 것과 동일한 등록 키를 등록 키 필드에 입력합니다. 등록 키는 일회용 공유 암호입니다.

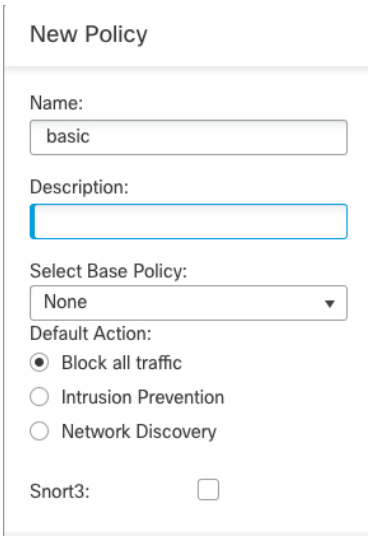
d) 다중 도메인 구축에서는 현재 도메인과 상관없이 디바이스를 리프 도메인으로 할당합니다.

   현재 도메인이 리프 도메인인 경우 디바이스는 자동으로 현재 도메인에 추가됩니다. 현재 도메인이 리프 도메인이 아닌 경우나 이후 재등록을 한 경우라면 리프 도메인으로 전환하여 디바이스를 구성합니다.

e) (선택 사항) 디바이스 그룹에 디바이스를 추가합니다.

f) 등록 시 디바이스를 구축하기 위해 초기 액세스 제어 정책을 선택하거나 새 정책을 생성합니다.

   새 정책을 생성하는 경우 기본 정책만 생성합니다. 나중에 필요에 따라 정책을 사용자 정의할 수 있습니다.



g) 디바이스에 적용할 라이선스를 선택합니다.

h) 디바이스 설정 중 NAT ID를 사용하는 경우 고급 섹션을 확장하고 고유 **NAT ID** 필드에 동일한 NAT ID를 입력합니다.

i) 패킷 전송 체크 박스를 선택하여 디바이스가 FMC에 패킷을 전송하도록 합니다.

이 옵션은 기본적으로 활성화되어 있습니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 FMC에 전송합니다. 이벤트를 비활성화하면 이벤트 정보는 FMC에 전송되지만 패킷 데이터는 전송되지 않습니다.

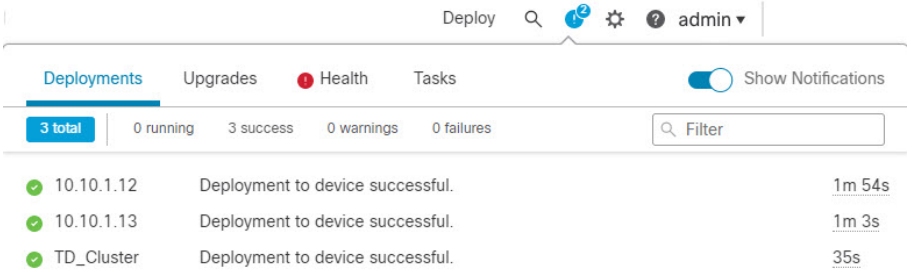
j) **Register(**등록**)**를 클릭합니다.

FMC은 제어 유닛을 식별해 등록하고 모든 데이터 유닛을 등록합니다. 제어 유닛이 성공적으로 등록되지 않는 경우 클러스터가 추가되지 않습니다. 클러스터가 섀시에 없거나 다른 연결 문제로 등록이 실패할 수 있습니다. 이 경우 클러스터 유닛 추가를 다시 시도하시기를 권장합니다.

디바이스 > 디바이스 관리 페이지에 클러스터 이름이 표시됩니다. 클러스터 유닛을 보려면 클러스터를 확장합니다.

현재 등록되는 유닛에는 로딩 아이콘이 표시됩니다.

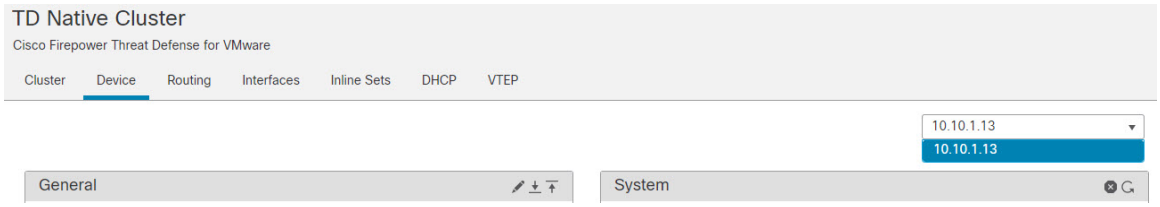
알림 아이콘을 클릭하고 작업을 선택하여 클러스터 유닛 등록을 모니터링할 수 있습니다. FMC은 각 유닛이 등록될 때마다 클러스터 등록 작업을 업데이트합니다. 유닛 등록에 실패하는 경우 클러스터 멤버 조정, 42 페이지의 내용을 참조하십시오.



단계 **2** 클러스터에 대해 **Edit(수정)** ( )을 클릭하여 디바이스별 설정을 구성합니다.

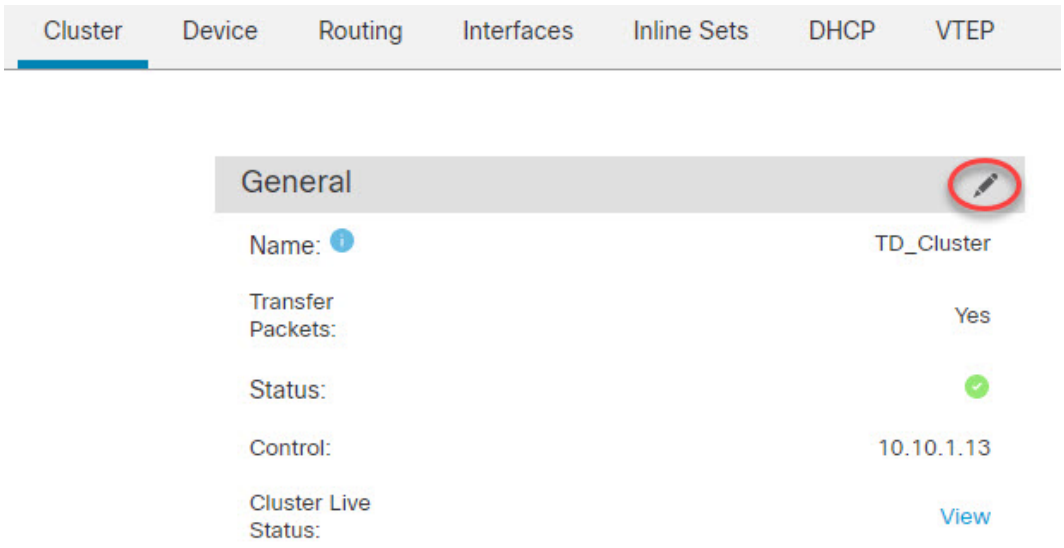
대부분의 구성은 클러스터의 멤버 유닛이 아닌 클러스터 전체에 적용할 수 있습니다. 예를 들어 유닛당 표시 이름을 변경할 수 있지만 전체 클러스터에 대해서만 인터페이스를 설정할 수 있습니다.

단계 **3** 디바이스 > 디바이스 관리 > 클러스터 화면에서 일반, 라이선스, 시스템및 상태 설정을 표시합니다.

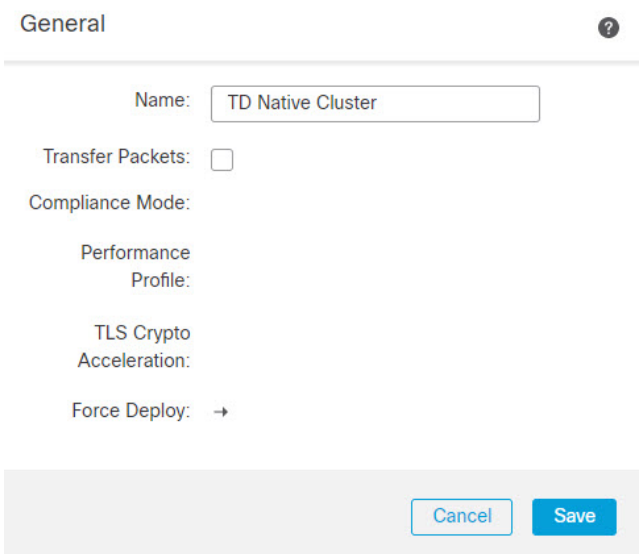


다음 클러스터별 항목을 참조하십시오.

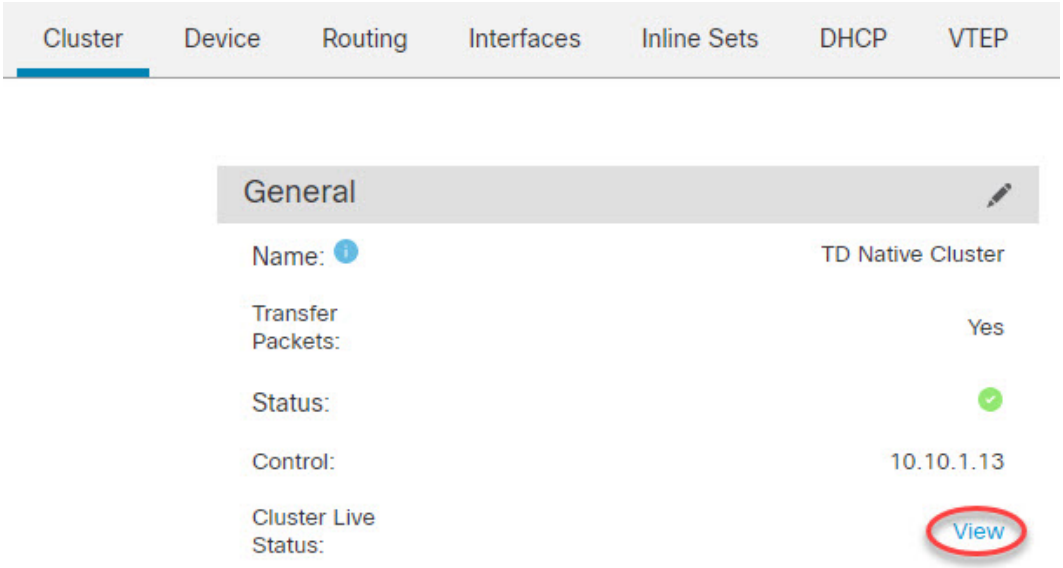
- **General (일반)> Name (이름) - Edit(수정)** ( )를 클릭하여 클러스터 표시 이름을 변경합니다.



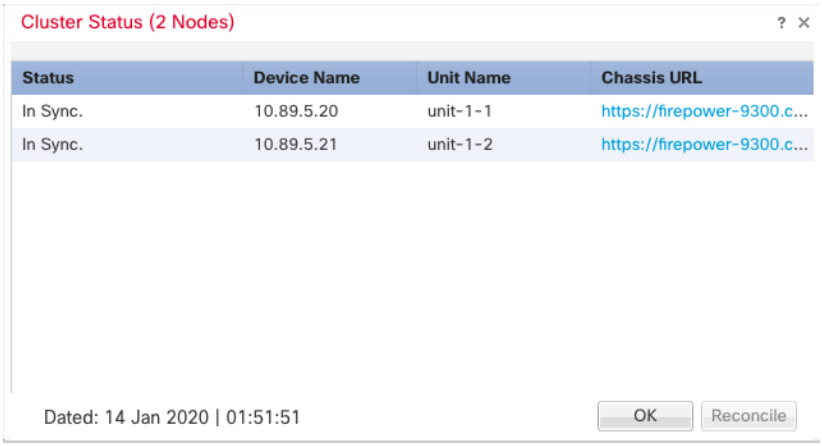
그런 다음 **Name(**이름**)** 필드를 설정합니다.



- **General(**일반**) > View cluster status(**클러스터 상태 보기**)**—**View cluster status(**클러스터 상태 보기**)** 링크를 클릭하여 **Cluster Status(**클러스터 상태**)** 대화 상자를 엽니다.



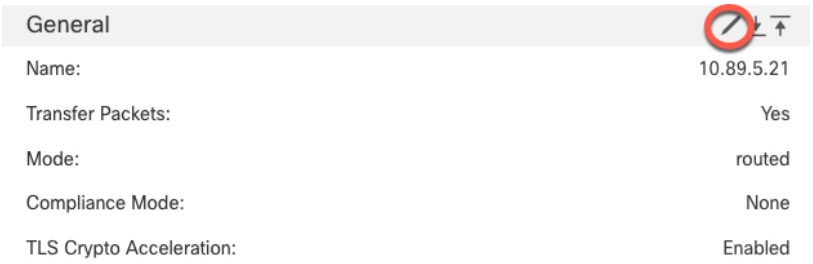
Cluster Status(클러스터 상태**)** 대화 상자에서 **Reconcile(**조정**)**을 클릭하면 데이터 유닛 등록을 다시 시도할 수도 있습니다.



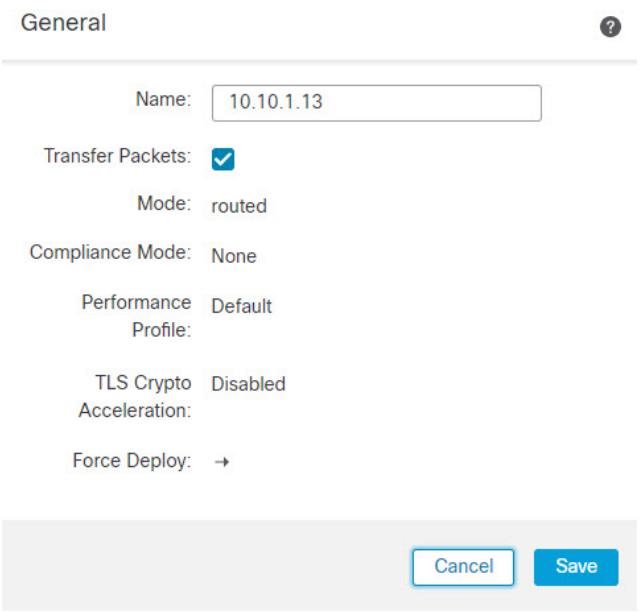
- **License(**라이선스**) - Edit(**수정**)** (✎)을 클릭하여 라이선스 등록을 설정할 수 있습니다.

단계 **4** **Devices(**디바이스**) > Device Management(**디바이스 관리**) >** 디바이스**(**디바이스**)**의 오른쪽 상단 드롭다운 메뉴에서 클러스터의 각 멤버를 선택하고 다음 설정을 구성할 수 있습니다.

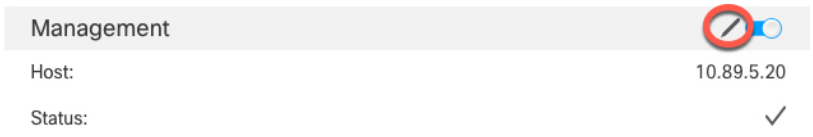
- **General(**일반**) > Name (**이름**) - Edit(**수정**)** (✎)을 클릭하여 클러스터 멤버 표시 이름을 변경합니다.



그런 다음 **Name(**이름**)** 필드를 설정합니다.



- **Management(**관리**) > Host(**호스트**)**—디바이스 설정에서 관리 IP 주소를 변경하는 경우 새 주소를 FMC에 일치시켜야 네트워크의 디바이스와 연결할 수 있습니다. **Management(**관리**)** 영역에서 **Host(**호스트**)** 주소를 편집합니다.



FMC: 클러스터, 데이터, 진단 인터페이스 구성

이 절차에서는 FXOS에서 클러스터를 구축할 때 클러스터에 할당한 각 데이터 인터페이스의 기본 파라미터를 구성합니다. 섀시 간 클러스터링의 경우, 데이터 인터페이스는 항상 Spanned EtherChannel 인터페이스입니다. 섀시 간 클러스터링을 위한 클러스터 제어 링크 인터페이스의 경우 MTU를 기본값에서 늘려야 합니다. 개별 인터페이스로 실행할 수 있는 유일한 인터페이스인 진단 인터페이스를 구성할 수도 있습니다.

참고 새시 간 클러스터링을 위해 Spanned EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 나타나지 않습니다. 이러한 요구 사항으로 인해 클러스터의 활성 유닛이 아닌 유닛에는 트래픽이 전달되지 않습니다.

프로시저

단계 **1** 디바이스 > 디바이스 관리를 선택하고 클러스터 옆의 **Edit(**수정**)** (✎)를 클릭합니다.

단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

단계 **3** 클러스터 제어 링크 구성

새시 간 클러스터링의 경우, 클러스터 제어 링크 MTU를 데이터 인터페이스의 최고 MTU보다 최소 100바이트 이상 높게 설정합니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다. MTU를 최댓값인 9184바이트로 설정하는 것이 좋습니다. 최솟값은 1400바이트입니다. 예를 들어 최대 MTU가 9184바이트이므로 가장 높은 데이터 인터페이스 MTU는 9084이 될 수 있는 반면, 클러스터 제어 링크는 9184로 설정할 수 있습니다.

기본 클러스터의 경우: 클러스터 제어 링크 인터페이스는 기본적으로 Port-Channel48입니다.

a) 클러스터 제어 링크 인터페이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다.
b) **General(**일반**)** 페이지의 **MTU** 필드에 1400에서 9184 사이의 값을 입력합니다. 최대값인 9184를 사용하는 것이 좋습니다.
c) **OK(**확인**)**를 클릭합니다.

단계 **4** 데이터 인터페이스 구성

a) (선택 사항) 데이터 인터페이스에 VLAN 하위 인터페이스를 구성합니다. 이 절차의 나머지는 하위 인터페이스에 적용됩니다. 하위 인터페이스 추가를 참조하십시오.
b) 데이터 인터페이스를 위해 **Edit(**수정**)** (✎)을 클릭합니다.
c) 라우팅 모드 인터페이스 구성 또는 에 따라 이름, IP 주소 및 기타 파라미터브리지 그룹 인터페이스 구성를 구성하십시오.

참고 클러스터 제어 링크 인터페이스 MTU가 데이터 인터페이스 MTU보다 최소 100바이트 이상 높지 않으면 데이터 인터페이스의 MTU를 줄여야 한다는 오류가 표시됩니다. 클러스터 제어 링크 MTU를 늘리려면 단계 3, 34 페이지의 내용을 참조하십시오. 그 후에는 계속해서 데이터 인터페이스를 구성할 수 있습니다.

d) 새시 간 클러스터의 경우 EtherChannel의 수동 전역 MAC 주소를 설정합니다. **Advanced(**고급**)**를 클릭해서 액티브 **MAC** 주소 필드에 H.H.H. 형식으로 MAC 주소를 입력합니다. 여기서 H는 16비트 16진수입니다.

예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다. 즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없습니다.

스탠바이 **MAC** 주소는 무시되므로 설정하지 마십시오.

잠재적인 네트워크 연결 문제를 방지하기 위해 Spanned EtherChannel에 대한 MAC 주소를 구성해야 합니다. 수동 구성된 MAC 주소를 사용할 경우, 해당 MAC 주소가 현재 제어 유닛에 유지됩니다. MAC 주소를 구성하지 않은 상태에서 제어 유닛을 변경하는 경우 새 제어 유닛에서는 인터페이스의 새 MAC 주소를 사용하며, 이로 인해 네트워크가 잠시 중단될 수 있습니다.

e) **OK(**확인**)**를 클릭합니다. 다른 데이터 인터페이스에 대해 위 단계를 반복합니다.

단계 **5** (선택 사항) 진단 인터페이스 구성

진단 인터페이스는 개별 인터페이스 모드에서 실행할 수 있는 유일한 인터페이스입니다. 예를 들어 시스템 로그 메시지 또는 SNMP에 이 인터페이스를 사용할 수 있습니다.

a) IPv4 및/또는 IPv6 주소 풀을 추가하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Address Pools(**주소 풀**)**을 선택합니다. 주소 풀를 참조하십시오.

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. 가상 IP 주소가 이 풀의 일부가 아니어도 동일한 네트워크에 있어야 합니다. 사전에 각 장치에 할당된 정확한 로컬 주소를 확인할 수 없습니다.

b) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**에서 진단 인터페이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다.

c) **IPv4**에서 **IP** 주소 및 마스크를 입력합니다. IP 주소는 현재 제어 유닛에 항상 속해 있는 클러스터의 고정 주소입니다.

d) **IPv4** 주소 풀 드롭다운 목록에서 생성한 주소 풀을 선택합니다.

e) **IPv6 >** 기본 탭의 **IPv6** 주소 풀 드롭다운 목록에서 생성한 주소 풀을 선택합니다.

f) 다른 인터페이스 설정은 기본으로 구성합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

FXOS: 클러스터 유닛 제거

다음 섹션에서는 클러스터에서 유닛을 일시적으로 또는 영구적으로 제거하는 방법을 설명합니다.

임시 제거

하드웨어나 네트워크 장애 등의 이유 때문에 클러스터 유닛이 클러스터에서 자동으로 제거됩니다. 이 제거는 조건을 수정할 때까지 임시로 적용되며, 클러스터에 다시 참여할 수 있습니다. 클러스터링을 수동으로 비활성화할 수도 있습니다.

디바이스가 현재 클러스터에 있는지 확인하려면, 애플리케이션에서 **show cluster info** 명령을 사용해 Firepower Chassis Manager **Logical Devices(**논리적 디바이스**)** 페이지:

FMC을(를) 사용하는 FTD의 경우에는 FMC 디바이스 목록에 디바이스를 남겨 두어야 클러스터링 재활성화 후 전체 기능을 다시 사용할 수 있습니다.

- 애플리케이션에서 클러스터링 비활성화 - 애플리케이션 CLI를 사용하여 클러스터링을 비활성화할 수 있습니다. **cluster remove unit** *name* 명령을 입력해 로그인한 유닛 외의 모든 유닛을 제거합니다. 부트스트랩 설정과 제어 유닛에서 동기화한 마지막 설정도 그대로 유지되므로 나중에 설정이 유실되는 일 없이 유닛을 다시 추가할 수 있습니다. 이 명령을 데이터 유닛에 입력해서 제어 유닛을 제거하면 새로운 제어 유닛이 선택됩니다.

  디바이스가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 부트스트랩 구성에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우에는 관리 인터페이스가 비활성화됩니다.

  클러스터링을 다시 활성화하려면 FTD에 **cluster enable**을(를) 입력합니다.

- 애플리케이션 인스턴스 비활성화 - **Logical Devices(**논리적 디바이스**)** 페이지의 Firepower Chassis Manager에서 슬라이더 활성화됨( )을(를) 클릭합니다. 나중에 슬라이더 비활성화됨( )을(를) 사용하여 다시 활성화할 수 있습니다.

- 보안 모듈/엔진 종료 - **Security Module/Engine(**보안 모듈/엔진**)** 페이지의 Firepower Chassis Manager에서 전원 끄기 아이콘을 클릭합니다.

- 섀시 종료 - **Overview(**개요**)** 페이지의 Firepower Chassis Manager에서 종료 아이콘을 클릭합니다.

영구 제거

다음 방법을 사용하면 클러스터 멤버를 영구적으로 제거할 수 있습니다.

FMC을(를) 사용하는 FTD의 경우, 섀시에서 클러스터링을 비활성화하면 유닛을 FMC 디바이스 목록에서 제거해야 합니다.

- 논리적 디바이스 삭제 - **Logical Devices(**논리적 디바이스**)** 페이지의 Firepower Chassis Manager에서 삭제( )을(를) 클릭합니다. 이제 독립형 논리적 디바이스, 새 클러스터를 구축하거나 동일한 클러스터에 새 논리적 디바이스를 추가할 수 있습니다.

- 서비스에서 섀시 또는 보안 모듈 제거- 서비스에서 디바이스를 제거하면, 교체 하드웨어를 클러스터의 새 멤버로 추가할 수 있습니다.

FMC: 클러스터 멤버 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 멤버를 관리할 수 있습니다.

새 클러스터 멤버 추가

FXOS에서 새 클러스터 멤버를 추가할 때 Firepower Management Center에서는 멤버를 자동으로 추가합니다.

시작하기 전에

- 인터페이스 구성은 다른 섀시의 교체 유닛과 동일해야 합니다.

프로시저

단계 **1** FXOS에서 클러스터에 새 장치를 추가합니다. FXOS 설정 가이드를 참조하십시오.

새 유닛이 클러스터에 추가될 때까지 기다립니다. 클러스터 상태를 보려면 Firepower 섀시 관리자의 논리적 디바이스 화면을 참조하거나 Firepower Threat Defense **show cluster info** 명령어를 사용하십시오.

단계 **2** 새 클러스터 멤버는 자동으로 추가됩니다. 교체 유닛 등록을 모니터링하려면 다음을 확인합니다.

- **Cluster Status(**클러스터 상태**)** 대화 상자(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) 아이콘 또는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 탭 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크)—섀시의 클러스터에 등록 중인 장치는 "클러스터 등록 중"이 표시됩니다. 클러스터에 참가한 후 FMC이 등록을 시도하며 상태가 "등록 사용 가능"으로 변경됩니다. 등록이 완료되면 상태가 "동기화 중"으로 변경됩니다. 등록에 실패하는 경우 유닛은 "등록 사용 가능" 상태가 유지됩니다. 이 경우 조정을 클릭하여 강제로 다시 등록합니다.
- 시스템 상태 아이콘 > **Task(**작업**)** - FMC는 모든 등록 이벤트 및 오류를 표시합니다.
- 디바이스 > 디바이스 관리 - 디바이스 목록 페이지에서 클러스터를 확장하면 유닛이 등록될 때 왼쪽에 로딩 아이콘이 표시되는 것을 볼 수 있습니다.

클러스터 멤버 교체

기존 클러스터에서 클러스터 멤버를 추가하거나 교체합니다. FMC은 교체 유닛을 자동으로 감지합니다. 하지만 FMC의 기존 클러스터 멤버를 수동으로 삭제해야 합니다. 이 절차는 다시 초기화하는 유닛에도 적용됩니다. 이 경우 하드웨어는 동일하지만 새로운 멤버로 표시됩니다.

시작하기 전에

- 인터페이스 구성은 다른 섀시의 교체 유닛과 동일해야 합니다.

프로시저

단계 **1** 가능한 경우, 새로운 섀시에 FXOS의 이전 섀시에 대한 설정을 백업하고 복원합니다.

Firepower 9300에서 모듈을 교체하는 경우 이 단계를 수행할 필요가 없습니다.

기존 섀시에 백업 FXOS 컨피그레이션이 없는 경우 새 클러스터 멤버 추가, 37 페이지의 단계를 먼저 수행합니다.

아래 단계에 대한 자세한 정보는 FXOS 환경 설정 가이드를 참조하십시오.

a) Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정이 포함된 XML 파일을 내보내려면 구성 내보내기 기능을 사용합니다.
b) 교체 섀시에 설정 파일을 가져옵니다.
c) 라이선스 계약에 동의합니다.
d) 필요한 경우 클러스터의 나머지와 일치하도록 논리적 디바이스 애플리케이션의 인스턴스 버전을 업그레이드합니다.

단계 **2** 이전 유닛의 FMC에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) > **Delete(**삭제**)**을 클릭합니다.

단계 **3** 유닛을 삭제하려면 확인합니다.

유닛이 클러스터 및 FMC 디바이스 리스트에서 삭제됩니다.

단계 **4** 신규 또는 새로 초기화된 클러스터 멤버는 자동으로 추가됩니다. 교체 유닛 등록을 모니터링하려면 다음을 확인합니다.

- **Cluster Status(**클러스터 상태**)** 대화 상자(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) 아이콘 또는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크)—섀시의 클러스터에 등록 중인 장치는 "클러스터 등록 중"이 표시됩니다. 클러스터에 참가한 후 FMC

이 등록을 시도하며 상태가 "등록 사용 가능"으로 변경됩니다. 등록이 완료되면 상태가 "동기화 중"으로 변경됩니다. 등록에 실패하는 경우 유닛은 "등록 사용 가능" 상태가 유지됩니다. 이 경우 **Reconcile(조정) All(전부)**을 클릭하여 강제로 다시 등록합니다.

- 시스템 ( ) > **Tasks(작업)** - FMC는 모든 등록 이벤트 및 오류를 표시합니다.
- 디바이스 > 디바이스 관리 - 디바이스 목록 페이지에서 클러스터를 확장하면 유닛이 등록될 때 왼쪽에 로딩 아이콘이 표시되는 것을 볼 수 있습니다.

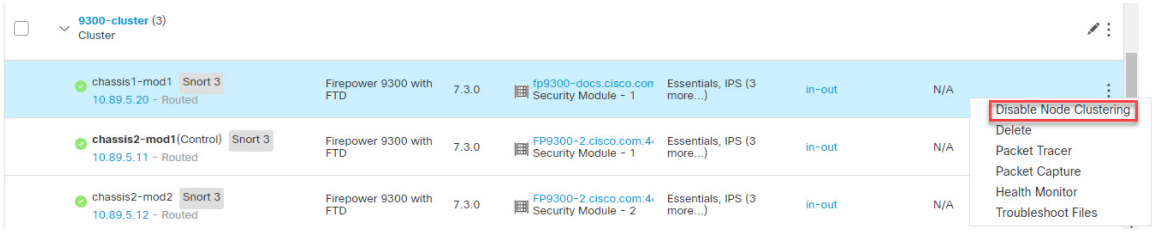
멤버 비활성화

유닛 삭제를 준비하거나 유지 보수를 위해 일시적으로 멤버를 비활성화할 수 있습니다. 이 절차는 멤버를 일시적으로 비활성화하기 위함이며, FMC 디바이스 목록에 유닛을 유지해야 합니다.

참고 유닛이 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 부트스트랩 구성에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우 관리 인터페이스가 비활성화됩니다. 추가 구성을 하려면 콘솔을 사용해야 합니다.

프로시저

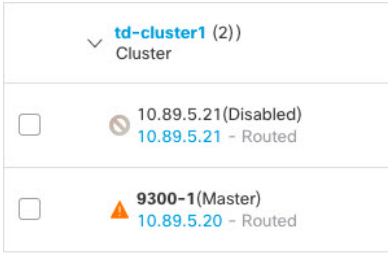
단계 **1** 비활성화하려는 유닛에 대해 **Devices(디바이스)** > **Device Management(디바이스 관리)** 추가 ( ) **Disable Clustering(클러스터링 비활성화)**을 선택합니다.



Cluster Status(클러스터 상태) 대화 상자(**Devices(디바이스)** > **Device Management(디바이스 관리)** > 추가 ( ) > **Cluster Live Status(클러스터 라이브 상태)**)에서 유닛을 비활성화할 수도 있습니다.

단계 **2** 유닛에서 클러스터링을 비활성화하고자 함을 확인합니다.

유닛이 **Devices(디바이스)** > **Device Management(디바이스 관리)** 목록에서 그 이름 옆에 **(Disabled(비활성화 됨))**로 표시됩니다.



단계 **3** 클러스터링을 다시 활성화하려면 클러스터 재참가, 40 페이지의 내용을 참조하십시오.

클러스터 재참가

예를 들어 인터페이스 오류 등으로 유닛이 클러스터에서 제거되거나 수동으로 클러스터링을 비활성화한 경우 클러스터를 다시 참가시킬 수 있습니다. 클러스터 다시 조인을 시도하기 전에 오류가 해결되었는지 확인하십시오. 유닛이 클러스터에서 제거되는 이유에 대한 자세한 내용은 클러스터 다시 참가, 58 페이지을 참조하십시오.

프로시저

단계 **1** 다시 활성화하려는 유닛에 대해 **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택하고 추가 (⋮) **Enable Clustering(**클러스터링 다시 활성화**)**을 선택합니다.

Cluster Status(클러스터 상태**)** 대화 상자**(Devices(**디바이스**) > Device Management(**디바이스 관리**) >** 추가 (⋮) **> Cluster Live Status(**클러스터 라이브 상태**))**에서 유닛을 다시 활성화할 수도 있습니다.

단계 **2** 유닛에서 클러스터링을 활성화할지 확인합니다.

데이터 유닛 삭제

클러스터 멤버를 영구적으로 제거해야 한다면(예를 들어 Firepower 9300에서 모듈, 섀시를 제거하는 경우) FMC에서 삭제해야 합니다.

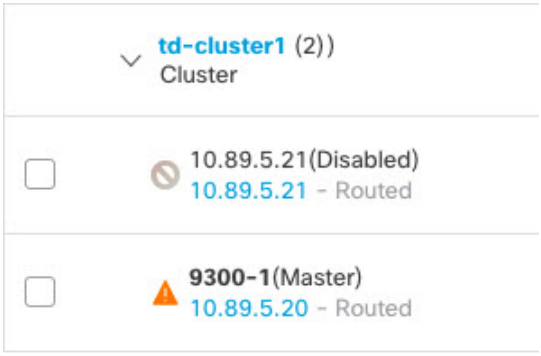
클러스터의 정상 부분에 해당하거나, 멤버를 임시로 비활성화하고 싶다면 멤버를 삭제해선 안 됩니다. FXOS의 클러스터에서 영구적으로 삭제하는 방법은 FXOS: 클러스터 유닛 제거, 35 페이지의 내용을 참조하십시오. FMC에서 제거했지만 여전히 클러스터에 속한다면 트래픽을 계속 전달하며, FMC에서는 관리할 수 없는 제어 유닛이 될 수도 있습니다.

시작하기 전에

수동으로 유닛을 비활성화하려면 멤버 비활성화, 39 페이지의 내용을 참조하십시오. 유닛을 삭제하기 전에 수동으로 또는 상태 장애로 인해 유닛이 비활성 상태여야 합니다.

프로시저

단계 **1** FMC에서 유닛이 삭제될 수 있는지 확인합니다.**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 유닛에 **(Disabled (**비활성화됨**))**가 표시되는지 확인합니다.



추가 (⋮)의 **Cluster Status(**클러스터 상태**)** 대화 상자에서 각 유닛의 상태를 확인할 수도 있습니다. 상태가 변하지 않는 경우 **Cluster Status(**클러스터 상태**)** 대화 상자에서 **Reconcile All(**모두 조정**)**을 클릭하여 강제로 업데이트합니다.

단계 **2** 데이터 유닛의 FMC에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) > **Delete(**삭제**)**을 클릭합니다.

단계 **3** 유닛을 삭제하려면 확인합니다.

유닛이 클러스터 및 FMC 디바이스 리스트에서 삭제됩니다.

제어 유닛 변경

주의 제어 유닛을 변경하는 가장 좋은 방법은 제어 유닛의 클러스터링을 비활성화한 후 새 제어가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 제어 유닛이 될 정확한 유닛을 지정해야 할 경우, 이 섹션의 절차를 참조하십시오. 중앙 집중식 기능의 경우 제어 유닛을 강제로 변경하면 모든 연결이 취소되며 새 제어 유닛에서 연결을 다시 설정해야 합니다.

제어 유닛을 변경하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮)> **Cluster Live Status(**클러스터 라이브 상태**)**를 선택하여 **Cluster Status(**클러스터 상태**)** 대화 상자를 엽니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크에서 **Cluster Status(**클러스터 상태**)** 대화 상자에 액세스할 수도 있습니다.

단계 **2** 제어 유닛이 될 유닛에 대해 추가 (⋮) **Change Role to Control(**역할을 제어로 변경**)**을 선택합니다.

단계 **3** 역할 변경을 확인하라는 메시지가 표시됩니다. 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

클러스터 멤버 조정

클러스터 멤버 등록에 실패하면 섀시에서 Firepower Management Center에 대해 클러스터 멤버십을 다시 조정합니다. 예를 들어, FMC이 특정 프로세스 중이거나 네트워크에 문제가 있는 경우, 데이터 유닛 등록에 실패할 수 있습니다.

프로시저

단계 **1** 클러스터에 대해 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 추가 (⋮)를 선택한 다음 **Cluster Live Status(**클러스터 라이브 상태**)**를 선택하여 **Cluster Status(**클러스터 상태**)** 대화 상자를 엽니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크에서 **Cluster Status(**클러스터 상태**)** 대화 상자를 열 수도 있습니다.

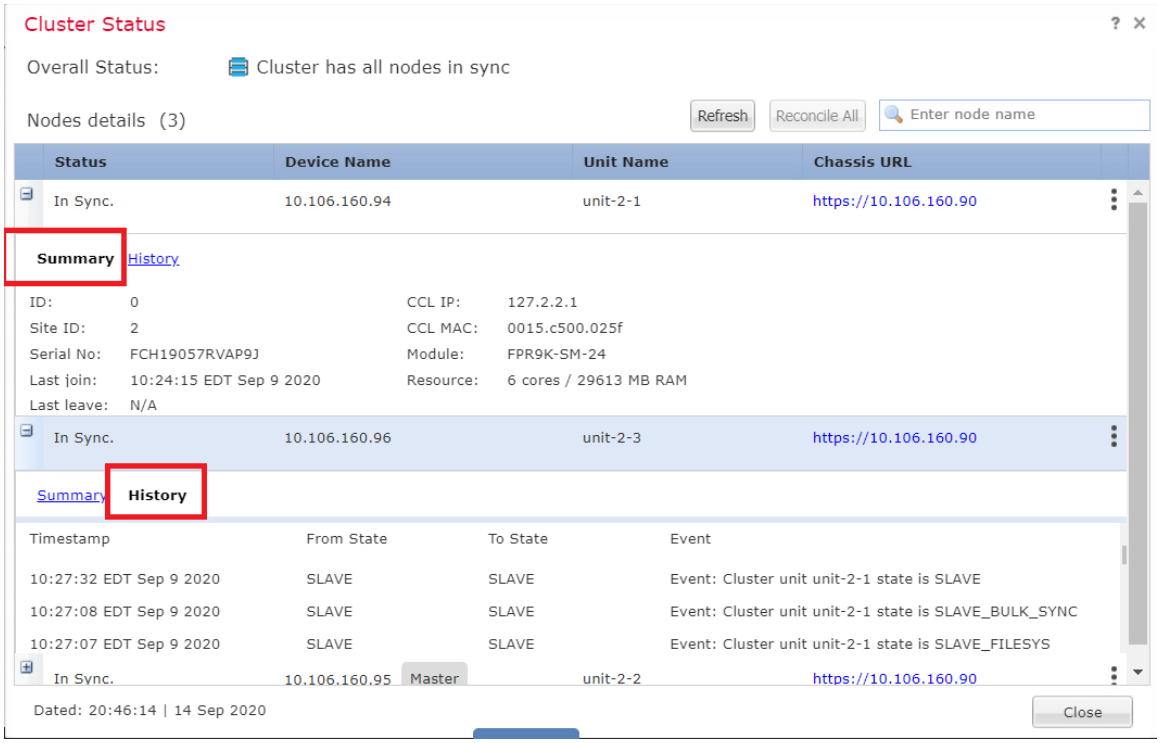
단계 **2** **Reconcile(**조정**)All(**모두**)**을 클릭합니다.

클러스터 상대에 대한 자세한 내용은 FMC: 클러스터 모니터링, 43 페이지을 참고하십시오.

FMC: 클러스터 모니터링

Firepower Management Center과 FTD CLI에서 클러스터를 모니터링할 수 있습니다.

- **Cluster Status(**클러스터 상태**)** 대화 상자는 **Devices(**디바이스**)** > **Device Management** > 추가 (⋮) 아이콘 또는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)**에서 제공됩니다.



제어 유닛에는 역할을 식별하는 그래픽 표시기가 있습니다.

클러스터 멤버 상태에는 다음 상태가 포함됩니다.

- 동기화 중 - 유닛이 FMC에 등록되었습니다.
- 등록 보류 중 - 유닛이 클러스터의 일부이지만 아직 FMC에 등록되지 않았습니다. 유닛 등록에 실패하는 경우, **Reconcile(**조정**)All(**모두**)**을 클릭하여 등록을 다시 시도할 수 있습니다.
- 클러스터링이 비활성화됨 - 유닛이 FMC에 등록되었지만, 클러스터의 비활성 멤버입니다. 클러스터링 구성은 나중에 다시 활성화하려는 경우에도 그대로 유지됩니다. 또는 클러스터에서 유닛을 삭제할 수 있습니다.
- 클러스터 참가 중... - 유닛이 섀시의 클러스터에 참가 중이지만 아직 참가가 완료되지 않았습니다. 참가가 끝나면 FMC로 등록합니다.

각 유닛에 대해 요약 또는 기록을 볼 수 있습니다.

추가 (⋮) 메뉴의 각 유닛에 대해 다음 상태 변경을 수행할 수 있습니다.

- 클러스터링 비활성화
- 클러스터링 활성화
- 역할을 제어로 변경

- 시스템 ( ) > **Tasks(**작업**)** 페이지로 이동합니다.

  Tasks(작업**)** 페이지는 각 유닛 등록에 대한 클러스터 등록 작업의 업데이트를 보여줍니다.

- 디바이스 > 디바이스 관리 > *cluster_name*입니다.

  디바이스 목록 페이지에서 클러스터를 확장하는 경우, IP 주소 옆에 해당 역할과 함께 표시되는 제어 유닛을 포함하여 모든 멤버 유닛을 볼 수 있습니다. 아직 등록 중인 유닛은 로딩 아이콘이 표시됩니다.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  전체 클러스터에 대한 집계된 데이터 또는 다른 정보를 보려면 **show cluster** 명령을 사용합니다.

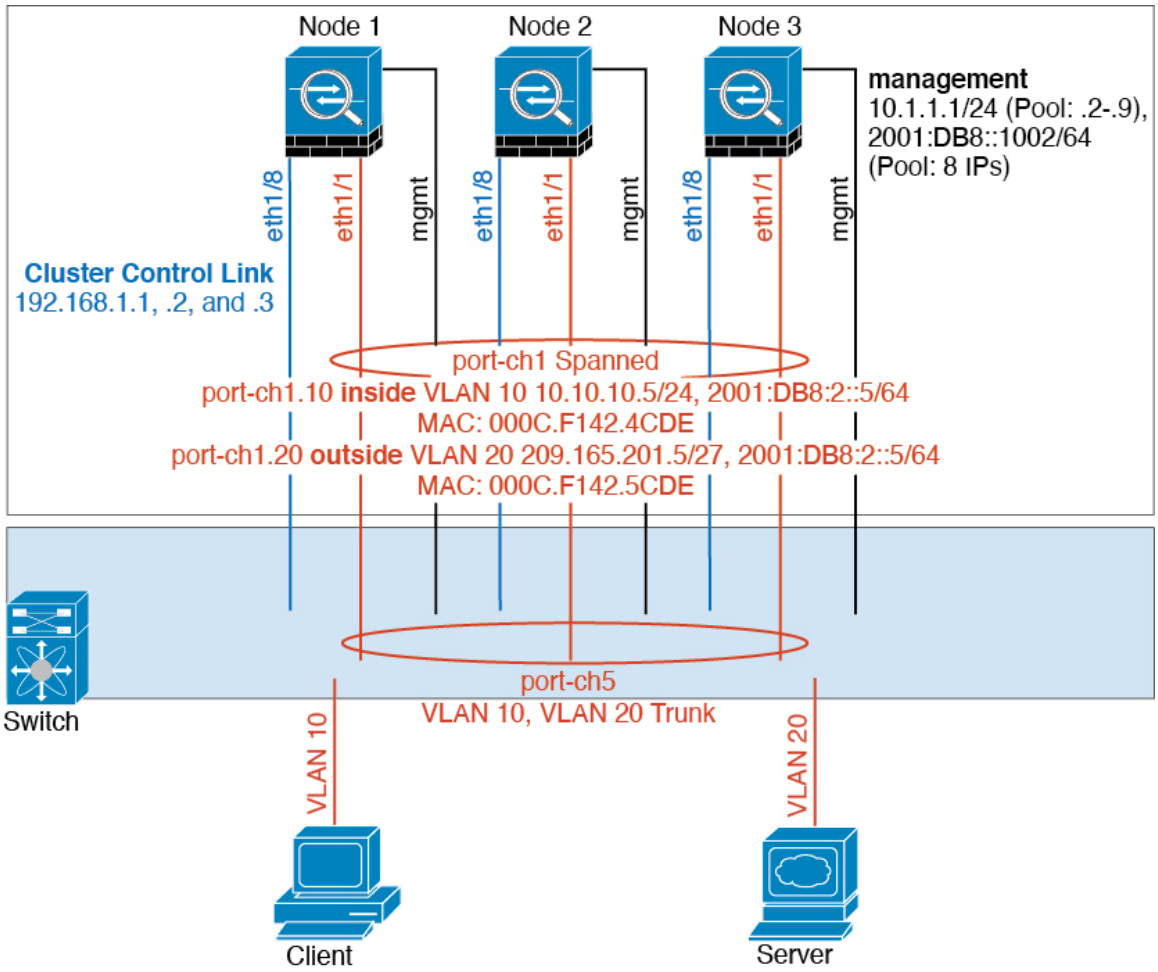
- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  클러스터 정보를 보려면 **show cluster info** 명령을 사용합니다.

클러스터링의 예

이러한 예에는 일반적인 구축이 포함됩니다.

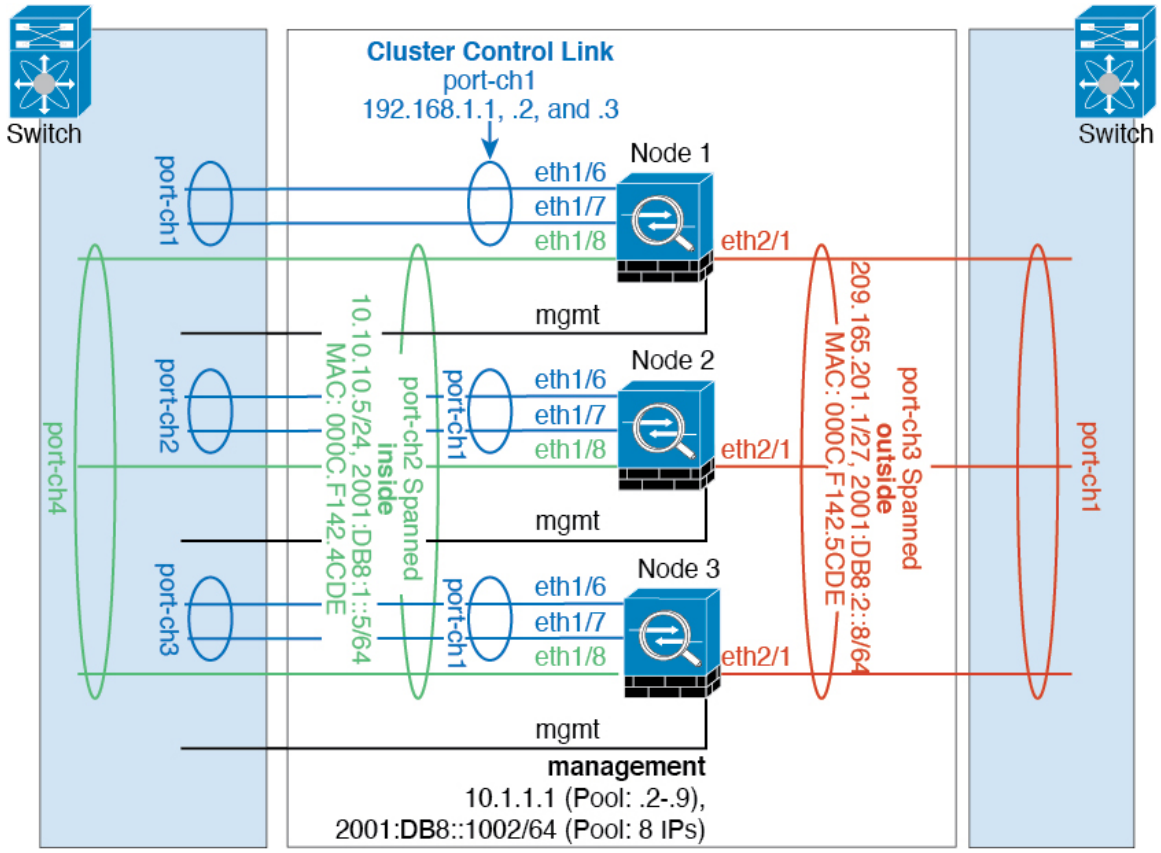
단일화된 방화벽



서로 다른 보안 도메인의 데이터 트래픽은 서로 다른 VLAN에 연결됩니다. 예를 들어, VLAN 10은 내부 네트워크용이고 VLAN 20은 외부 네트워크용입니다. 각 에는 외부 스위치 또는 라우터에 연결된 하나의 물리적 포트가 있습니다. 트렁킹이 활성화되어 있으므로 물리적 링크의 모든 패킷은 캡슐화된 802.1q입니다. 는 VLAN 10과 VLAN 20 사이의 방화벽입니다.

스팬 EtherChannel을 사용할 경우, 모든 데이터 링크가 스위치 측의 단일한 EtherChannel로 그룹화됩니다. 를 사용할 수 없게 될 경우, 스위치에서 나머지 유닛 간의 트래픽을 리밸런싱합니다.

트래픽 분리

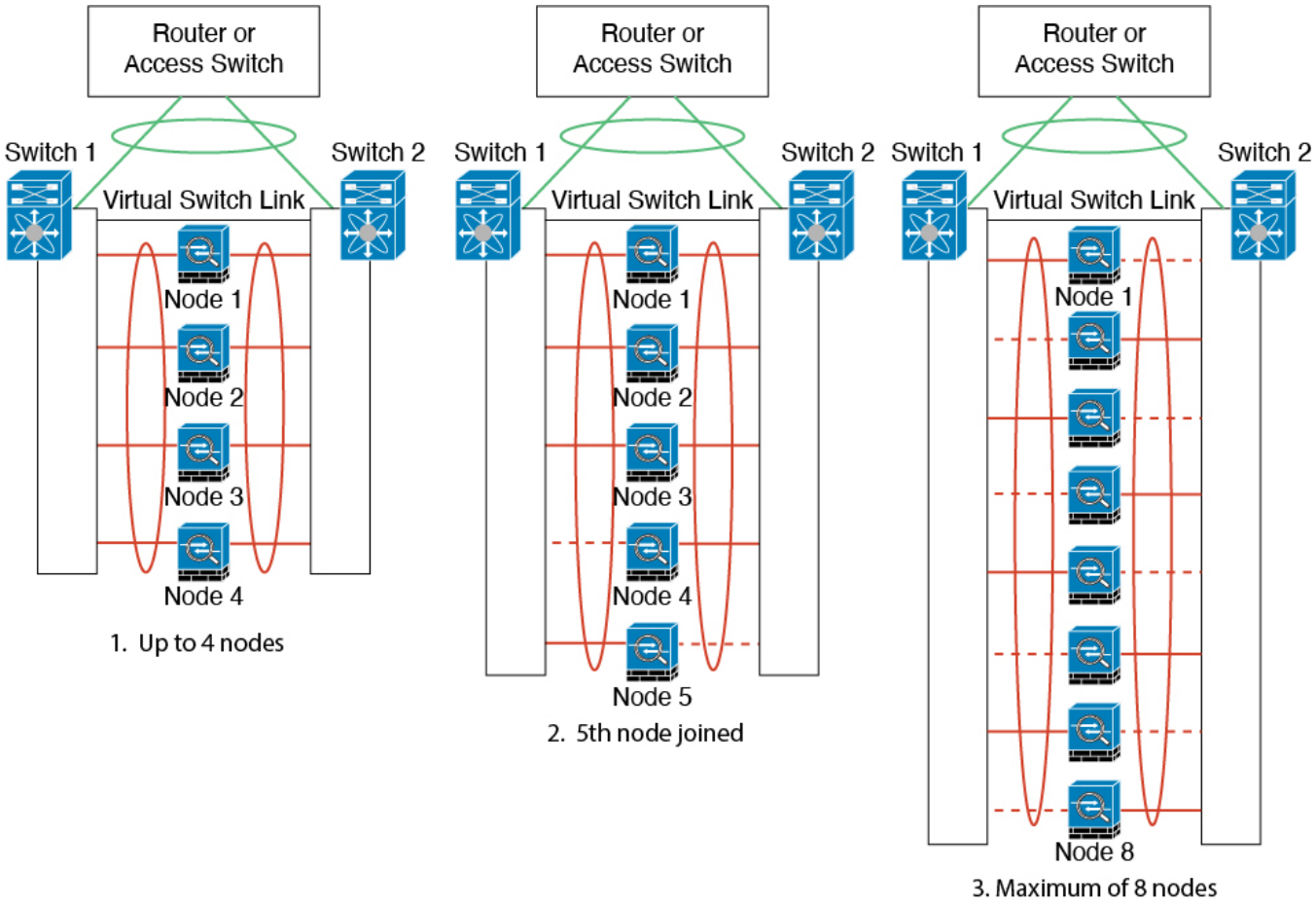


내부 네트워크와 외부 네트워크 간의 트래픽을 물리적으로 분리하려는 경우가 있습니다.

위의 다이어그램에 표시된 것과 같이, 왼쪽에는 내부 스위치에 연결되는 스팬 EtherChannel이 하나 있고 오른쪽에는 외부 스위치에 연결되는 스팬 EtherChannel이 있습니다. 필요한 경우 각 EtherChannel에 VLAN 하위 인터페이스를 생성할 수도 있습니다.

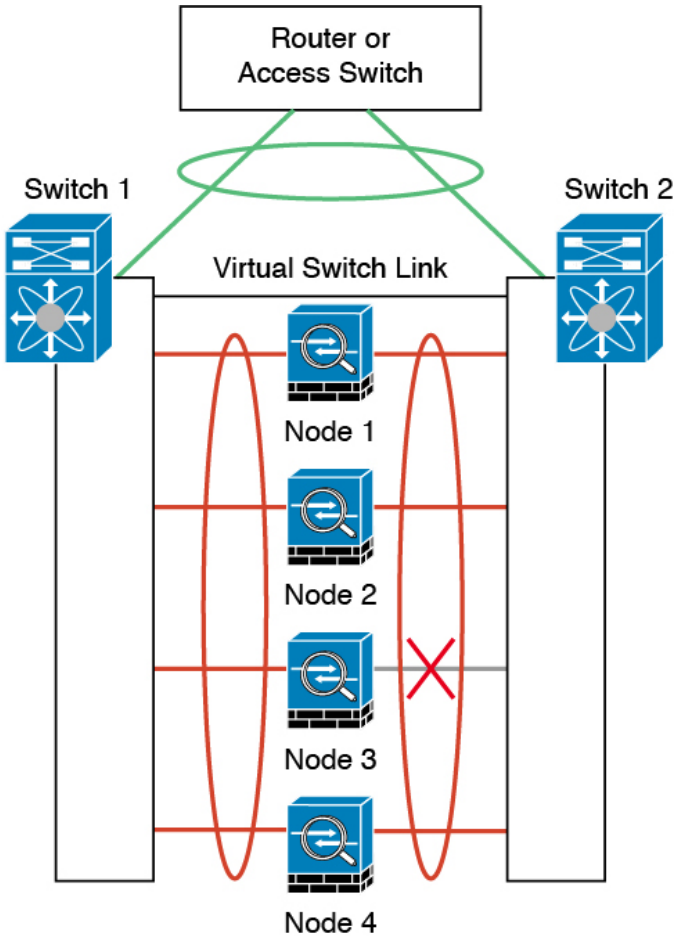
백업 링크가 포함된 스팬 **EtherChannel**(기존 **8** 액티브 포트/**8** 스탠바이)

기존 EtherChannel에서 활성 포트의 최대 개수는 스위치 측에서 8개로 제한됩니다. 8-유닛 클러스터가 있을 경우 유닛당 2개의 포트를 EtherChannel에 할당하며, 이렇게 하면 총 16개의 전체 포트 중 8개는 스탠바이 모드가 되어야 합니다. FTD에서는 LACP를 사용하여 어떤 링크를 활성화하거나 스탠바이 상태로 설정해야 하는지 협상을 수행합니다. VSS 또는 vPC를 사용하여 다중 스위치 EtherChannel을 활성화할 경우 스위치 간 이중화를 실현할 수 있습니다. FTD의 모든 물리적 포트는 우선 슬롯 번호를 기준으로, 그다음에는 포트 번호를 기준으로 순서가 지정됩니다. 다음 그림에서 순서가 낮은 포트는 "제어" 포트(예: Ethernet 1/1)이고 다른 포트는 "데이터" 포트(예: Ethernet 1/2)입니다. 하드웨어 연결은 대칭을 이루어야 합니다. 모든 제어 링크는 하나의 스위치에서 종료되어야 하며, 모든 데이터 링크는 VSS/vPC가 사용된 경우 다른 스위치에서 종료되어야 합니다. 다음 다이어그램에서는 클러스터에 참가하는 유닛의 수가 증가하여 링크의 총 개수가 증가할 경우 어떤 상황이 발생하는지 보여 줍니다.

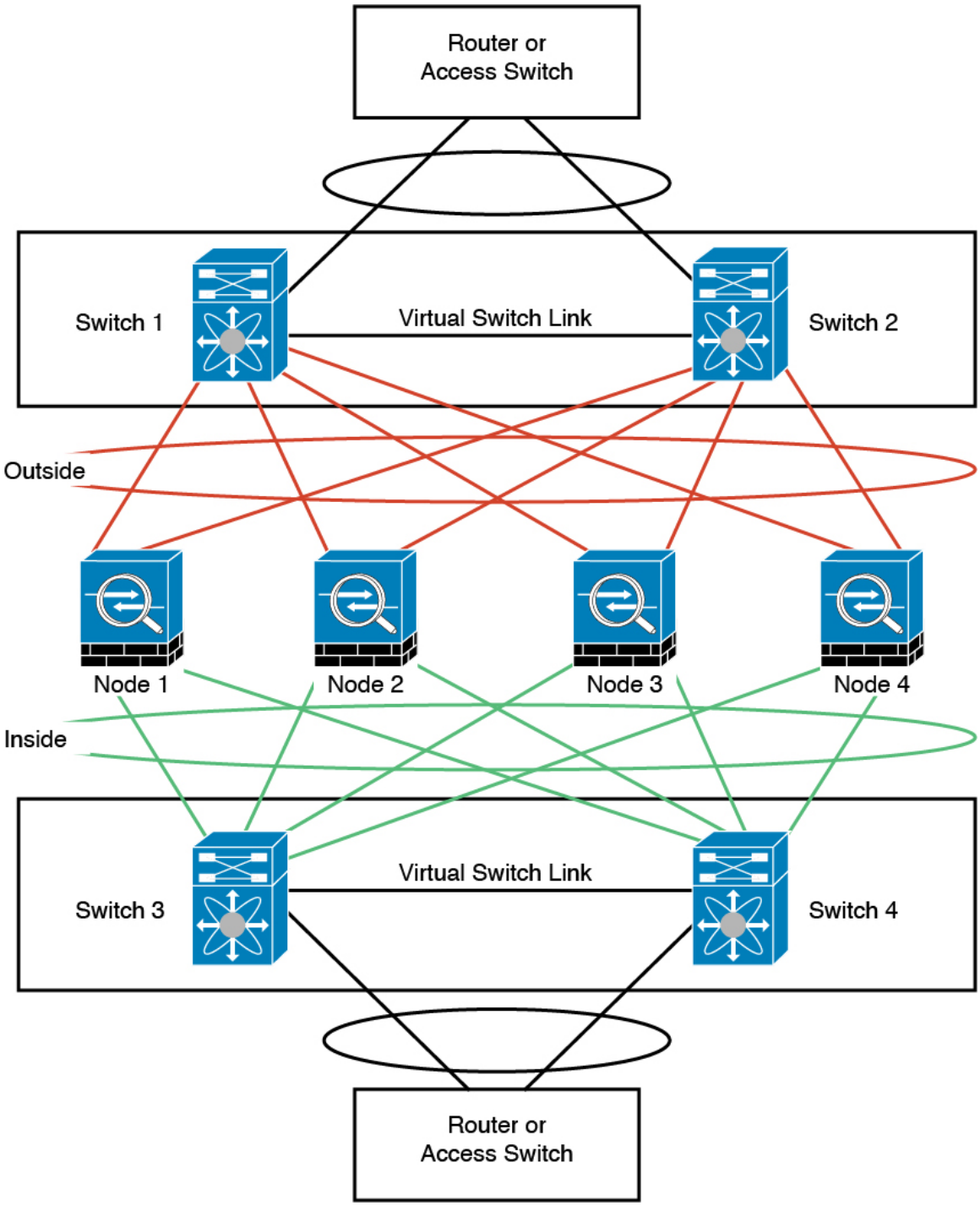


원칙은 우선 채널에 있는 액티브 포트의 수를 최대화하고, 그다음에는 액티브 제어 포트의 수와 액티브 데이터 포트의 수가 균형을 이루도록 유지하는 것입니다. 클러스터에 5번째 유닛이 참가할 경우 모든 유닛 간의 트래픽이 균일하게 조정되지 않습니다.

링크 또는 디바이스 오류는 이와 동일한 원칙에 따라 처리됩니다. 또한 완벽하지 않은 로드 밸런싱 상황에 처하게 될 수 있습니다. 다음 그림에는 유닛 중 하나에 단일 링크 오류가 발생한 4-유닛 클러스터가 나와 있습니다.



네트워크에는 여러 개의 EtherChannel이 구성될 수 있습니다. 다음 다이어그램에는 내부의 EtherChannel과 외부의 EtherChannel이 나와 있습니다. 한쪽 EtherChannel의 제어 및 데이터 링크에 모두 오류가 발생할 경우 클러스터에서 FTD가 제거됩니다. 이렇게 되면 외부 네트워크와 내부 네트워크의 연결이 이미 끊긴 경우, 외부 네트워크의 트래픽이 FTD에 전달되지 않습니다.



클러스터링에 대한 참조

이 섹션에는 클러스터링이 작동하는 방식에 대한 자세한 정보가 포함되어 있습니다.

FTD 기능 및 클러스터링

일부 FTD 기능은 클러스터링이 지원되지 않으며, 일부 기능은 기본 유닛에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

클러스터링으로 지원되지 않는 기능

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.

참고 클러스터링으로도 지원되지 않는 FlexConfig 기능(예: WCCP 검사)을 보려면 ASA 일반 운영 설정 가이드를 참조하십시오. FlexConfig를 사용하면 FMC GUI에 없는 여러 ASA 기능을 설정할 수 있습니다. FlexConfig 정책의 내용을 참조하십시오.

- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- DHCP 클라이언트, 서버, 프록시 DHCP 릴레이가 지원됩니다.
- Virtual Tunnel Interface(VTI)
- 고가용성
- 통합 라우팅 및 브리징
- FMC UCAPL/CC 모드

클러스터링을 위한 중앙 집중식 기능

다음 기능은 제어 노드에서만 지원되며 클러스터에 확장되지 않습니다.

참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 노드에서 제어 노드로 전달됩니다.

리밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 제어 노드로 리밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 제어 노드로 다시 전송됩니다.

중앙 집중식 기능의 경우 제어 노드에 오류가 발생하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다.

참고 클러스터링으로도 집중되는 FlexConfig 기능(예: RADIUS 검사)을 보려면 ASA 일반 운영 설정 가이드를 참조하십시오. FlexConfig를 사용하면 FMC GUI에 없는 여러 ASA 기능을 설정할 수 있습니다. FlexConfig 정책의 내용을 참조하십시오.

- 다음과 같은 애플리케이션 감시:

- DCERPC
- ESMTP
- NetBIOS
- PPTP
- RSH
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 고정 경로 모니터링
- 사이트 간 VPN
- IGMP 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- PIM 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- 동적 라우팅

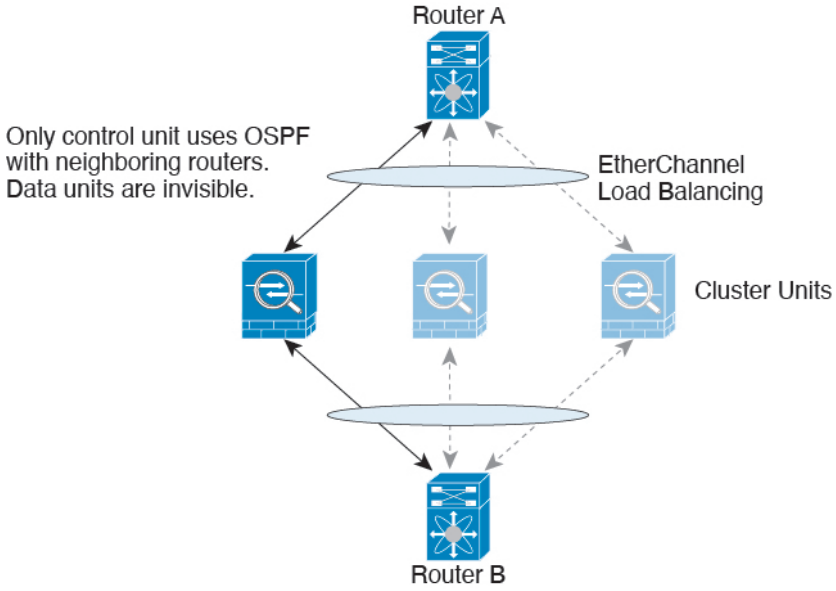
연결 설정

연결 제한은 클러스터 전체에서 시행됩니다. 각 노드에는 브로드캐스트 메시지를 기반으로 한 클러스터 전체의 카운터 값이 표시됩니다. 효율성을 고려하여 클러스터 전체에 구성된 연결 제한이 제한 수에 정확하게 적용되지 않을 수 있습니다. 각 노드는 언제든지 클러스터 전체 카운터 값을 과대 평가하거나 과소 평가할 수 있습니다. 그러나 로드 밸런싱된 클러스터에서는 시간이 지남에 따라 정보가 업데이트됩니다.

동적 라우팅 및 클러스터링

라우팅 프로세스는 제어 유닛에서만 실행되며, 경로는 제어 유닛을 통해 파악되고 보조 유닛에 복제됩니다. 라우팅 패킷이 데이터 유닛에 전송되면 해당 패킷은 제어 유닛에 리디렉션됩니다.

그림 5: 동적 라우팅



데이터 유닛이 제어 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 제어 유닛에서 데이터 유닛으로 동기화되지 않습니다. 제어 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 흐름을 소유한 경우, 데이터 채널 소유자 유닛에서는 유휴 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유휴 시간 제한 값을 업데이트합니다. 그러나 제어 흐름 소유자가 다시 로드되고 제어 흐름이 다시 호스팅된 경우, 부모/자식 흐름 관계가 더 이상 유지되지 않으며 제어 흐름 유휴 시간 제한도 업데이트되지 않습니다.

멀티캐스트 라우팅 및 클러스터링

제어 유닛에서는 fast-path 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 처리합니다. 연결이 설정되면 각 데이터 유닛에서 멀티캐스트 데이터 패킷을 전달할 수 있습니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 FTD에 전송할 수 있습니다. 패킷이 NAT 소유자가 아닌 FTD에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에

게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다. 보안 및 정책 확인 결과에 따라 NAT 소유자가 패킷에 대해 연결을 생성하지 않을 수 있으므로 수신 노드는 소유자에 대한 전달 플로우를 생성하지 않습니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
  - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 노드에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서 호스트의 트래픽이 3개 노드 모두에 로드 밸런싱되는 경우 각 노드에 하나씩 3개의 블록이 할당될 수 있습니다.
  - 백업 풀의 백업 노드에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
  - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 새 풀이 작동하게 되는 동안 여전히 전환 중이던 xlate 백업 요청에 대해 xlate 백업 생성이 실패하게 됩니다. 이러한 동작은 포트 블록 할당 기능과 관련이 없으며, 풀이 분산되고 트래픽이 클러스터 노드 전체에서 부하 분산되는 클러스터 구축 과정에서만 발생하는 일시적인 PAT 풀 문제입니다.
  - 클러스터에서 작업할 때는 단순히 블록 할당 크기를 변경할 수 없습니다. 새 크기는 클러스터에서 각 디바이스를 다시 로드한 후에만 적용됩니다. 각 디바이스를 다시 로드하지 않으려면 모든 블록 할당 규칙을 삭제하고 해당 규칙과 관련된 모든 xlate를 지우는 것이 좋습니다. 그런 다음 블록 크기를 변경하고 블록 할당 규칙을 다시 생성할 수 있습니다.
- 동적 PAT에 대한 NAT 풀 주소 분산 - PAT 풀을 구성하면 클러스터는 풀의 각 IP 주소를 포트 블록으로 나눕니다. 기본적으로 각 블록은 512포트이지만 포트 블록 할당 규칙을 구성하는 경우에는 블록 설정이 대신 사용됩니다. 이러한 블록은 클러스터의 노드 간에 균등하게 분산되므로 각 노드에는 PAT 풀의 각 IP 주소에 대해 하나 이상의 블록이 있습니다. 따라서 예상되는 PAT 처리된 연결 수에 충분한 경우 클러스터의 PAT 풀에 IP 주소를 하나만 포함할 수 있습니다. PAT 풀 NAT 규칙에 예약된 포트 1~1023을 포함하도록 옵션을 구성하지 않는 한 포트 블록은 1024~65535 포트 범위를 포함합니다.
- 여러 규칙에서 PAT 풀 재사용 - 여러 규칙에서 동일한 PAT 풀을 사용하려면 규칙에서 인터페이스 선택에 주의해야 합니다. 모든 규칙에서 특정 인터페이스를 사용하거나 또는 모든 규칙에서 "any(임의의)"를 사용해야 합니다. 규칙 전체에서 특정 인터페이스와 "any(임의의)"를 혼합할 수 없거나, 시스템에서 클러스터의 오른쪽 노드에 대한 반환 트래픽을 일치시키지 못할 수 있습니다. 규칙 당 고유한 PAT 풀을 사용하는 것은 가장 신뢰할 수 있는 옵션입니다.
- 라운드 로빈 없음 — 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 확장 PAT 없음 - 클러스터링에서 확장 PAT가 지원되지 않습니다.
- 제어 노드에 의해 관리되는 동적 NAT xlate — 제어 노드에서는 xlate 테이블을 유지하고 데이터 노드에 복제합니다. 동적 NAT가 필요한 연결이 데이터 노드에 전달되고 xlate가 테이블에 없을 경우, 제어 노드에서 xlate를 요청합니다. 데이터 노드에서는 이 연결을 소유합니다.

- 오래된 xlates - 연결 소유자의 xlate 유휴 시간이 업데이트되지 않습니다. 따라서 유휴 시간이 유휴 시간 제한을 초과할 수 있습니다. refcnt가 0인 구성된 시간 초과 값보다 큰 유휴 타이머 값은 오래된 xlate를 나타냅니다.
- 다음을 검사할 수 있는 고정 PAT 없음
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 10,000개가 넘는 매우 많은 NAT 규칙이 있는 경우 디바이스 CLI에서 **asp rule-engine transactional-commit nat** 명령을 사용하여 트랜잭션 커밋 모델을 활성화해야 합니다. 그렇지 않으면 노드가 클러스터에 조인하지 못할 수 있습니다.

SIP 검사 및 클러스터링

로드 밸런싱으로 인해 모든 노드에서 제어 플로우를 만들 수 있지만 하위 데이터 플로우는 동일한 노드에 상주해야 합니다.

SNMP 및 클러스터링

SNMP 에이전트에서는 진단 인터페이스 로컬 IP 주소로 각각의 개별 FTD를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 제어 노드가 선택된 경우, 새 제어 노드에 대한 폴링이 이루어지지 않습니다.

클러스터링과 함께 SNMPv3를 사용할 때 초기 클러스터 형성 후 새 클러스터 노드를 추가하면 SNMPv3 사용자가 새 노드에 복제되지 않습니다. 사용자를 제거하고 다시 추가한 다음 사용자가 새 노드에 복제하도록 강제로 구성을 재구축해야 합니다.

Syslog 및 클러스터링

- 클러스터의 각 노드에서는 고유한 syslog 메시지를 생성합니다. 각 노드에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 구성은 클러스터의 모든 노드에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 노드에서는 단일 노드에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 구성에 할당된 로컬-노드 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, syslog 메시지는 다른 노드에서 생성된 것처럼 보입니다.

TLS/SSL 연결 및 클러스터링

TLS/SSL 연결의 암호 해독된 상태는 동기화되지 않습니다. 연결 소유자 장애가 발생하는 경우, 암호 해독된 연결이 재설정됩니다. 새 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.

Cisco TrustSec 및 클러스터링

제어 노드에서만 보안 그룹 태그(SGT) 정보를 학습합니다. 그런 다음 제어 노드에서는 SGT를 데이터 노드에 제공하며, 데이터 노드에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

VPN 및 클러스터링

사이트 간 VPN은 중앙 집중식 기능이며, 마스터 유닛에서만 VPN 연결을 지원합니다.

참고 원격 액세스 VPN은 클러스터링으로 지원되지 않습니다.

VPN 기능은 마스터 유닛에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 제어 유닛에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 제어 유닛이 선택되면 VPN 연결을 다시 설정해야 합니다.

VPN 터널을 스팬 인터페이스 주소에 연결할 경우 연결이 제어 유닛에 자동으로 전달됩니다.

VPN 관련 키 및 인증서는 모든 유닛에 복제됩니다.

성능 확장 요소

클러스터에 여러 유닛을 결합할 경우 총 클러스터 성능을 대략 다음과 같이 예측할 수 있습니다.

- 통합 TCP 또는 CPS 처리량의 80%
- 통합 UDP 처리량의 90%
- 트래픽 조합에 따라 통합된 EMIX(이더넷 MIX) 처리량의 60%

예를 들어 TCP 처리량의 경우 3개의 SM-44 모듈이 있는 Firepower 9300은 단독으로 실행하면 실제 방화벽 트래픽 중 약 135Gbps를 처리할 수 있습니다. 2개의 섀시의 경우 최대 통합 처리량은 270Gbps(2개 섀시 x 135Gbps)의 약 80%인 216Gbps입니다.

제어 유닛 선택

클러스터의 멤버는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 제어 '유닛을 선택합니다.

1. 클러스터를 구축할 때 각 유닛은 3초마다 선택 요청을 브로드캐스트합니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 클러스터를 구축할 때 설정되며 구성 불가능합니다.

3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 제어 유닛이 됩니다.

참고 가장 우선순위가 높은 유닛이 공동으로 여러 개인 경우, 클러스터 유닛 이름과 일련 번호를 사용하여 제어 유닛을 결정합니다.

4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 제어 유닛이 되는 것은 아닙니다. 기존 제어 유닛은 응답이 중지되지 않는 한 항상 제어 유닛으로 유지되며 응답이 중지될 때에 새 제어 유닛이 선택됩니다.

5. 제어 유닛이 일시적으로 여러 개 있는 "스플릿 브레인" 시나리오에서는 우선 순위가 가장 높은 유닛이 역할을 유지하는 반면 다른 유닛은 데이터 유닛 역할로 돌아갑니다.

참고 유닛을 수동으로 강제 변경하여 제어 유닛이 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 제어 유닛을 강제로 변경하면 모든 연결이 취소되며 새 제어 유닛에서 연결을 다시 설정해야 합니다.

클러스터 내의 고가용성

클러스터링에서는 섀시, 유닛 및 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

섀시 애플리케이션 모니터링

섀시 애플리케이션 상태 모니터링은 항상 활성화되어 있습니다. Firepower 4100/9300 섀시 수퍼바이저는 FTD 애플리케이션을 주기적으로(1초마다) 검사합니다. FTD 디바이스가 작동 중인데 Firepower 4100/9300 섀시 수퍼바이저와 3초 동안 통신할 수 없는 경우, FTD 디바이스에서는 syslog 메시지를 생성하고 클러스터를 떠납니다.

Firepower 4100/9300 섀시 수퍼바이저가 45초 후에 애플리케이션과 통신할 수 없는 경우, FTD 디바이스를 다시 로드합니다. FTD 디바이스가 수퍼바이저와 통신할 수 없는 경우, 클러스터에서 자신을 제거합니다.

유닛 상태 모니터링

각 유닛은 클러스터 제어 링크를 통해 브로드 캐스트 keepalive 하트 비트 패킷을 주기적으로 전송합니다. 제어 유닛이 시간 초과 기간 내에 데이터 유닛에서 keepalive 하트 비트 패킷 또는 기타 패킷을 수신하지 않는 경우, 제어 유닛은 클러스터에서 데이터 유닛을 제거합니다. 데이터 유닛이 제어 유닛에서 패킷을 수신하지 않으면 나머지 제어 멤버에서 새 제어 유닛이 선택됩니다.

네트워크 장애로 인해 유닛이 실제로 장애가 발생한 것이 아니라 클러스터 제어 링크를 통해 유닛이 서로 연결할 수 없는 경우, 클러스터는 격리된 데이터 유닛이 자체 제어 유닛을 선택하는 "스플릿 브레인" 시나리오로 전환될 수 있습니다. 예를 들어 두 클러스터 위치 간에 라우터가 실패하면 위치 1의 원래 제어 유닛이 클러스터에서 위치 2 데이터 유닛을 제거합니다. 한편, 위치 2의 유닛은 자체 제어

유닛을 선택하고 자체 클러스터를 구성합니다. 이 시나리오에서는 비대칭 트래픽이 실패할 수 있습니다. 클러스터 제어 링크가 복원되면 우선 순위가 더 높은 제어 장치가 제어 장치의 역할을 유지합니다. 자세한 내용은 제어 유닛 선택, 55 페이지를 참조하십시오.

인터페이스 모니터링

각 노드에서는 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 제어 노드에 보고합니다. 섀시 간 클러스터링의 경우 Spanned EtherChannel은 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 섀시에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인하고 인터페이스가 작동 중단 상태인지 FTD 애플리케이션에 정보를 제공합니다. 물리적 인터페이스가 모니터링됩니다(EtherChannel 인터페이스에 대한 기본 EtherChannel 포함). 작동 상태인 명명된 인터페이스만 모니터링 대상이 될 수 있습니다. 예를 들어, EtherChannel의 모든 멤버 포트는 명명된 EtherChannel이 클러스터에서 제거되기 전에 장애가 발생해야 합니다.

모니터링되는 인터페이스가 특정 노드에서 실패하지만 다른 노드에서는 활성 상태인 경우 해당 노드는 클러스터에서 제거됩니다. FTD 디바이스에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 해당 노드가 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. FTD 디바이스에서는 노드가 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 FTD 디바이스가 클러스터에서 제거되지 않습니다. 구성된 멤버의 경우 노드는 500밀리초 후에 제거됩니다.

섀시 간 클러스터링의 경우 클러스터에서 EtherChannel을 추가 또는 삭제하는 경우 인터페이스 상태 모니터링은 각 섀시의 변경을 확인할 수 있도록 95초간 일시 중단됩니다.

데코레이터 애플리케이션 모니터링

인터페이스에서 Radware DefensePro 애플리케이션과 같은 데코레이터 애플리케이션을 설치하는 경우, FTD 디바이스 및 데코레이터 애플리케이션 둘 다 클러스터에서 계속 작동해야 합니다. 유닛은 두 애플리케이션이 모두 작동할 때까지 클러스터에 참가하지 않습니다. 클러스터에 참가한 이후에 유닛은 3초마다 데코레이터 애플리케이션의 상태를 모니터링합니다. 데코레이터 애플리케이션이 작동하지 않으면 유닛이 클러스터에서 제거됩니다.

실패 이후 상태

클러스터의 노드에 오류가 발생할 경우, 해당 노드에서 호스팅하는 연결이 다른 노드로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 노드의 클러스터 제어 링크를 통해 공유됩니다.

제어 노드에 장애가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 제어 노드가 됩니다.

FTD는 실패 이벤트에 따라 클러스터에 다시 참가하려고 시도합니다.

참고 FTD가 비활성화되고 클러스터에 자동으로 다시 조인하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리/진단 인터페이스에서만 트래픽을 주고받을 수 있습니다.

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 최초 가입 시 오류가 발생한 클러스터 제어—클러스터 제어 링크의 문제를 해결한 다음 클러스터링을 다시 활성화하여 수동으로 클러스터를 다시 가입시켜야 합니다.
- 클러스터 가입 후 클러스터 제어 링크 장애 — FTD에서는 자동으로 5분마다 무기한으로 다시 가입하려고 시도합니다.
- 데이터 인터페이스 오류 — FTD에서는 5분에 다시 참가를 시도하며 그다음에는 10분, 마지막으로 20분에 참가를 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 FTD에서는 클러스터링을 비활성화합니다. 데이터 인터페이스의 문제를 해결한 다음 수동으로 클러스터링을 활성화해야 합니다.
- 노드 오류 — 노드 상태 검사 오류로 인해 클러스터에서 노드가 제거된 경우, 클러스터에 다시 참가할 수 있을지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한 경우 클러스터 제어 링크가 작동 상태이면 전원을 다시 가동할 때 노드가 클러스터에 다시 참가할 수 있습니다. FTD 애플리케이션은 5초마다 클러스터에 다시 참가하려고 시도합니다.
- 내부 오류 — 내부 장애 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등이 있습니다.
- 실패한 구성 구축-FMC에서 새 구성을 구축하는 경우 일부 클러스터 멤버에서는 구축이 실패하지만 다른 클러스터 멤버에서는 성공할 경우 실패한 노드는 클러스터에서 제거됩니다. 문제를 해결한 후 클러스터링을 다시 사용하도록 설정하여 클러스터에 수동으로 다시 참가해야 합니다. 제어 노드에서 구축이 실패하면 구축이 롤백되고 멤버가 제거되지 않습니다. 모든 데이터 노드에서 구축이 실패하면 구축이 롤백되고 멤버가 제거되지 않습니다.
- 섀시 애플리케이션 통신 장애 — FTD 애플리케이션에서 섀시 애플리케이션 상태가 복구되었는지 탐지할 경우, 클러스터에 자동으로 다시 참가하려고 시도합니다.

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 장애 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다. 백업 소유자는 일반적으로 관리자이기도 합니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 ***1:*** 클러스터 전반에 걸쳐 복제된 기능

트래픽	상태 지원	참고
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	—

트래픽	상태 지원	참고
MAC 주소 테이블	예	—
사용자 ID	예	—
IPv6 네이버 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—

클러스터에서 연결을 관리하는 방법

클러스터의 여러 노드에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

연결 역할

각 연결에 대해 정의된 다음 역할을 참조하십시오.

- 소유자 - 일반적으로 연결을 가장 처음 수신하는 노드입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다. 원래 소유자가 실패하고 새 노드가 연결에서 패킷을 수신하면, 관리자는 해당 노드로부터 새 소유자를 선택합니다.
- 백업 소유자 - 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있도록 소유자로부터 수신한 TCP/UDP 상태 정보를 저장하는 노드입니다. 백업 소유자는 장애 발생 시 연결을 승계할 수 없습니다. 소유자를 사용할 수 없는 경우, 연결에서 (로드 밸런싱을 기준으로) 패킷을 받을 첫 번째 노드가 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

  관리자(아래 설명 참조)는 소유자와 같은 노드가 아니라면 백업 소유자로도 사용됩니다. 소유자가 자신을 관리자로 선택하면 별도의 백업 소유자가 선택됩니다.

  Firepower 9300의 클러스터링(섀시 하나에 클러스터 노드가 3개까지 포함될 수 있음)에서 백업 소유자가 소유자와 같은 섀시에 있으면 섀시 장애로부터 플로우를 보호하기 위해 다른 섀시에서 추가 백업 소유자가 선택됩니다.
- 관리자 - 전달자의 소유자 조회 요청을 처리하는 노드입니다. 소유자가 새 연결을 수신할 경우, 소유자 노드에서는 소스/대상 IP 주소와 포트의 해시를 기준으로 관리자를 선택하며 관리자에 메시지를 전송하여 새 연결을 등록합니다(아래에서 ICMP 해시 세부 정보 참조). 패킷이 소유자가 아닌 다른 노드에 전달될 경우, 해당 노드는 관리자에 어떤 노드가 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다. 관리자가 실패하면 소유자는 새 관리자를 선택합니다.

  관리자는 소유자와 같은 노드가 아니면 백업 소유자로도 사용됩니다(위의 설명 참조). 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  ICMP/ICMPv6 해시 세부 정보:

- 에코 패킷의 경우 소스 포트는 ICMP 식별자이고, 대상 포트는 0입니다.
- 응답 패킷의 경우 소스 포트는 0이고, 대상 포트는 ICMP 식별자입니다.
- 기타 패킷의 경우 소스 및 대상 포트가 모두 0입니다.

- 전달자 — 패킷을 소유자에 전달하는 노드입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 흐름을 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 시퀀스 임의 설정을 비활성화한 경우 SYN 쿠키는 사용되지 않으며, 책임자에게 쿼리해야 합니다.) DNS 및 ICMP 같이 짧은 흐름의 경우 쿼리 대신 전달자가 책임자에게 패킷을 즉시 전송하고 책임자가 소유자에게 전송합니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.

참고 클러스터링을 사용할 때는 TCP 시퀀스 임의 설정을 비활성화하지 않는 것이 좋습니다. SYN/ACK 패킷이 삭제될 수 있으므로 일부 TCP 세션이 설정되지 않을 가능성이 적습니다.

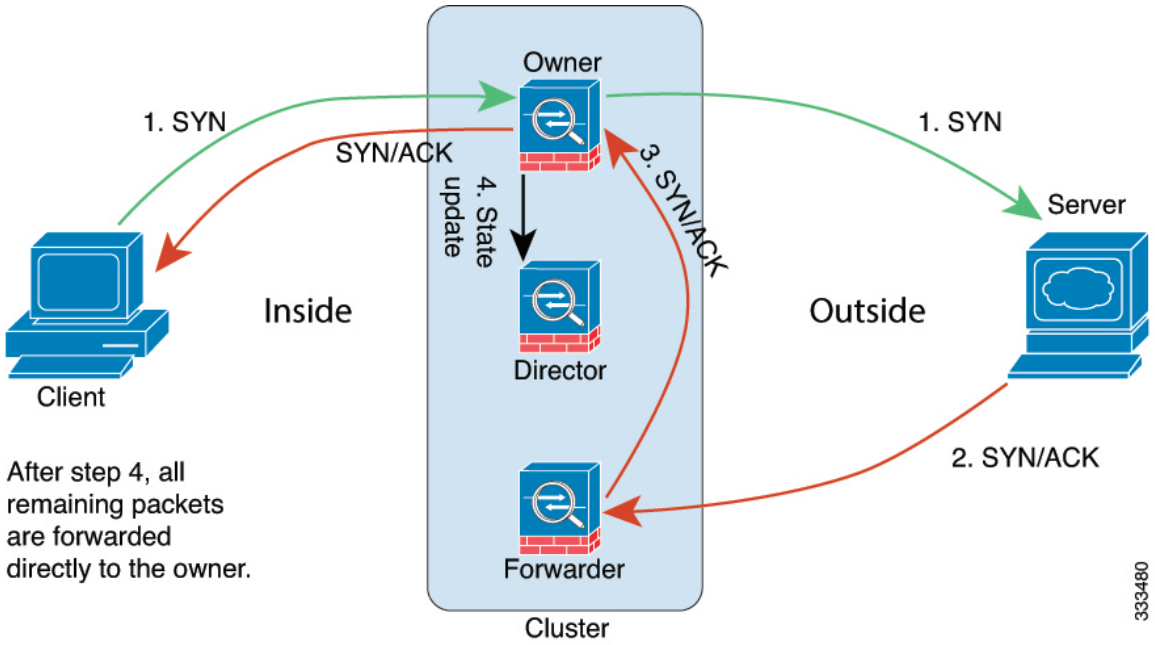
- 프래그먼트 소유자 - 프래그먼트화된 패킷의 경우 프래그먼트를 수신하는 클러스터 노드가 프래그먼트 소스 IP 주소, 대상 IP 주소 및 패킷 ID의 해시를 사용하여 프래그먼트 소유자를 결정합니다. 그런 다음 모든 프래그먼트가 클러스터 제어 링크를 통해 프래그먼트 소유자에게 전달됩니다. 첫 번째 프래그먼트만 스위치 로드 밸런싱 해시에 사용되는 5 튜플을 포함하기 때문에 프래그먼트는 다른 클러스터 노드로 로드 밸런싱될 수 있습니다. 다른 프래그먼트는 소스 및 대상 포트를 포함하지 않으며 다른 클러스터 노드에 로드 밸런싱될 수 있습니다. 프래그먼트 소유자는 패킷을 일시적으로 리어셈블하므로 소스/대상 IP 주소 및 포트의 해시를 기반으로 디렉터를 확인할 수 있습니다. 새 연결인 경우 프래그먼트 소유자가 연결 소유자로 등록됩니다. 기존 연결인 경우 프래그먼트 소유자는 클러스터 제어 링크를 통해 모든 프래그먼트를 제공된 연결 소유자에게 전달합니다. 그러면 연결 소유자가 모든 프래그먼트를 리어셈블합니다.

새 연결 소유권

로드 밸런싱을 통해 클러스터의 노드에 새 연결이 전송될 경우, 해당 노드에서는 연결의 양방향을 모두 소유합니다. 다른 노드에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 노드에 전달됩니다. 다른 노드에 반대 방향의 흐름이 전송될 경우, 이는 원래 노드로 다시 리디렉션됩니다.

TCP에 대한 샘플 데이터 플로우

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.

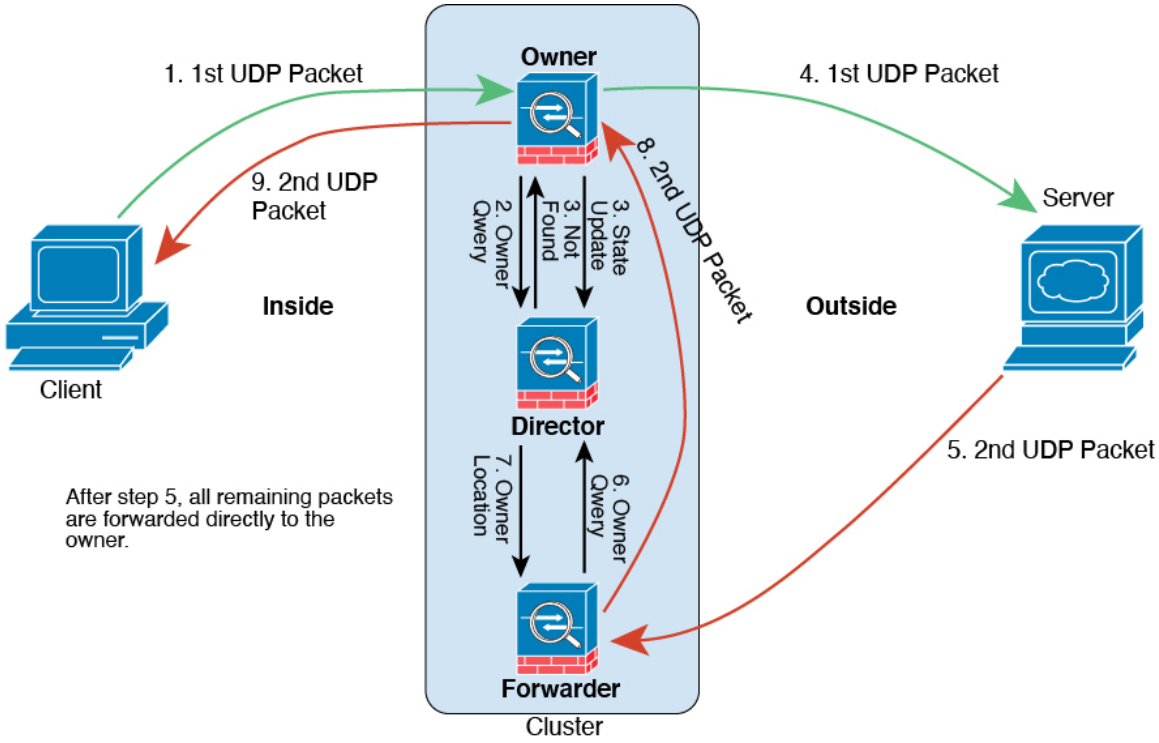


1. SYN 패킷은 클라이언트에서 시작되고 FTD에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 FTD에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 FTD는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.
5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 흐름을 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 노드에 전달된 경우, 관리자에 쿼리하고 플로우를 설정합니다.
8. 플로우 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

ICMP 및 UDP의 샘플 데이터 플로우

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.

1. 그림 ***6: ICMP*** 및 ***UDP*** 데이터 플로우



첫 번째 UDP 패킷은 클라이언트에서 시작되고 (로드 밸런싱 방법을 기준으로) FTD에 전달됩니다.

2. 첫 번째 패킷을 수신한 노드는 소스/대상 IP 주소 및 포트의 해시를 기반으로 선택된 관리자 노드에 쿼리합니다.
3. 관리자는 기존 플로우를 찾지 못하고 관리자 플로우를 생성하며 이전 노드로 패킷을 다시 전달합니다. 즉, 관리자가 이 플로우의 소유자를 선택했습니다.
4. 소유자가 플로우를 생성하고 관리자에게 상태 업데이트를 보내고 서버에 패킷을 전달합니다.
5. 두 번째 UDP 패킷은 서버에서 시작되어 전달자에게 전달됩니다.
6. 전달자는 관리자에게 소유권 정보를 쿼리합니다. DNS와 같이 짧은 플로우의 경우 쿼리하는 대신 전달자가 관리자에게 패킷을 즉시 전송하고 관리자가 소유자에게 전송합니다.
7. 관리자는 전달자에게 소유권 정보를 회신합니다.
8. 전달자는 전달 플로우를 생성하여 소유자 정보를 기록하고 소유자에게 패킷을 전달합니다.
9. 소유자는 패킷을 클라이언트에 전달합니다.

클러스터링 기록

기능	버전	세부 사항
방화벽 변경을 위한 클러스터 구축이 더 빠르게 완료됨	7.1	이제 방화벽 변경을 위한 클러스터 구축이 더 빠르게 완료됨 신규/수정된 화면: 없음
클러스터링을 위한 개선된 PAT 포트 블록 할당	7.0	개선된 PAT 포트 블록 할당을 통해 제어 유닛은 노드를 조인하기 위해 포트를 예약 상태로 유지하고 사용되지 않는 포트를 사전에 회수합니다. 할당을 최적화하기 위해 FlexConfig를 사용하는 **cluster-member-limit** 명령을 사용하여 클러스터에 포함할 최대 노드를 설정할 수 있습니다. 그러면 제어 유닛은 계획된 노드 수에 포트 블록을 할당할 수 있으며, 사용하지 않을 추가 노드에 대해 포트를 예약할 필요가 없습니다. 기본값은 16 노드입니다. syslog 747046을 모니터링하여 새 노드에 사용할 수 있는 포트가 충분한지 확인할 수도 있습니다. 신규/수정된 명령: **cluster-member-limit**(FlexConfig), **show nat pool cluster** [**summary**], **show nat pool ip detail**
Snort 변경에 대한 클러스터 구축이 더 빨리 완료되고 이벤트가있을 경우 더 빨리 실패합니다.	6.7	이제 Snort 변경을 위한 클러스터 구축이 더 빠르게 완료됨 또한 클러스터에 FMC 구축 실패를 초래하는 이벤트가 있을 경우 이제 장애가 더 빠르게 발생합니다. 신규/수정된 화면: 없음
FMC의 개선된 클러스터 관리	6.7	FMC에서는 이전에 CLI를 사용해야만 수행할 수 있었던 다음과 같은 클러스터 관리 기능을 개선했습니다. • 클러스터 유닛 활성화 및 비활성화 • 디바이스 관리 페이지에서 유닛별 히스토리 및 요약을 포함하여 클러스터 상태를 표시합니다. • 제어 유닛에 대한 역할 변경 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **More(**더 보기**)** 메뉴 • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크 **Cluster Status(**클러스터 상태**)** 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
다중 인스턴스 클러스터링	6.6	이제 컨테이너 인스턴스로 클러스터를 생성할 수 있습니다. Firepower 9300에서 클러스터의 각 모듈에 하나의 컨테이너 인스턴스를 포함해야 합니다. 보안 엔진/모듈마다 하나 이상의 컨테이너 인스턴스를 추가할 수 없습니다. 각 클러스터 인스턴스에 동일한 보안 모듈 또는 섀시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 신규/수정된 FXOS 명령: **set port-type cluster** 신규/수정된 Firepower Chassis Manager 화면: • 논리적 디바이스 > 클러스터 추가 • **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Add New(**새로 추가**)** 드롭다운 메뉴 **> Subinterface(**하위 인터페이스**) > Type(**유형**)** 필드 지원되는 플랫폼: Firepower 4100/9300의 FTD
병렬로 데이터 유닛에 구성 동기화	6.6	제어 유닛은 이제 기본적으로 구성 변경 사항을 데이터 유닛과 동시에 동기화합니다. 이전에는 동기화가 순차적으로 발생했습니다. 신규/수정된 화면: 없음
클러스터 가입 실패 또는 제거에 대한 메시지가 추가됨 **show cluster history**	6.6	클러스터 유닛이 클러스터에 조인하지 못하거나 클러스터를 떠나는 경우를 위한 새 메시지가 **show cluster history** 명령에 추가되었습니다. 신규/수정된 명령: **show cluster history** 신규/수정된 화면: 없음
DCD(Dead Connection Detection)의 이니시에이터 및 응답자 정보와, 클러스터에서의 DCD 지원입니다.	6.5	DCD(Dead Connection Detection)를 활성화하면, **show conn detail** 명령을 이용해 이니시에이터 및 응답자 정보를 얻을 수 있습니다. DCD(Dead Connection Detection)를 이용하면 비활성 연결을 유지할 수 있으며, **show conn** 출력은 엔드포인트를 얼마나 자주 조사했는지 알려줍니다. 또한 이제 DCD는 클러스터에서도 지원됩니다. 신규/수정된 명령: **show conn** (출력 전용) 지원되는 플랫폼: Firepower 4100/9300의 FTD

기능	버전	세부 사항
FMC에 개선된 FTD 클러스터 추가	6.3	이제는 FMC에 클러스터 유닛을 추가할 수 있으며 다른 클러스터 유닛은 자동으로 탐지됩니다. 이전에는 각 클러스터 유닛을 별도 디바이스로 추가한 뒤 관리 센터에서 클러스터로 그룹화해야 했습니다. 이제 클러스터 유닛 추가는 자동으로 진행됩니다. 유닛은 수동으로 삭제해야 합니다. 신규/수정된 화면: 디바이스 > 디바이스 관리> 추가 드롭다운 메뉴 > 디바이스 > 디바이스 추가 대화 상자 디바이스 > 디바이스 관리> 클러스터 탭 > 일반 영역 > 클러스터 등록 상태 > 현재 클러스터 요약 링크 > 클러스터 상태 대화 상자 지원되는 플랫폼: Firepower 4100/9300의 FTD
중앙 집중식 기능으로 클러스터링 Site-to-Site VPN 지원	6.2.3.3	이제 클러스터링 site-to-site VPN을 구성할 수 있습니다. 사이트 간 VPN은 중앙 집중식 기능이며, 마스터 유닛에서만 VPN 연결을 지원합니다. 지원되는 플랫폼: Firepower 4100/9300의 FTD
내부 오류 발생 후 클러스터에 자동으로 다시 조인	6.2.3	이전에는 많은 내부 오류 상태로 인해 클러스터에서 클러스터 유닛이 제거되었으며 문제를 해결한 후에 클러스터에 수동으로 다시 조인해야 했습니다. 이제 유닛은 자동으로 5분, 10분, 20분 간격으로 클러스터에 참가하려고 시도합니다. 내부 오류 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등 새/수정된 명령: 클러스터 정보 자동 연결 보기 수정된 화면이 없습니다. 지원되는 플랫폼: Firepower 4100/9300의 FTD

기능	버전	세부 사항
Firepower 4100은 6개 모듈을 위한 섀시 간 클러스터링을 지원합니다.	6.2	FXOS 2.1.1의 경우 이제 Firepower 9300 및 4100에서 섀시 간 클러스터링을 활성화할 수 있습니다. Firepower 9300의 경우에는 모듈을 6 개까지 포함할 수 있습니다. 예를 들어 섀시 6개에 모듈 1개, 섀시 3개에 모듈 2개, 또는 모듈을 6개까지 제공하는 어떤 조합도 사용할 수 있습니다. Firepower 4100의 경우에는 섀시를 6 개까지 포함할 수 있습니다. 참고 사이트 간 클러스터링은 지원되지 않습니다. 사이트별 MAC 및 IP 주소, 디렉터 현지화 , 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 맞춤화는 FlexConfig 기능을 사용하는 경우에만 구성 가능합니다. 수정된 화면이 없습니다. 지원되는 플랫폼: Firepower 4100/9300의 FTD
Firepower 9300을 위한 섀시 내 클러스터링	6.0.1	Firepower 9300 섀시 내에서 최대 3개의 보안 모듈을 클러스터링할 수 있습니다. 섀시의 모든 모듈은 클러스터에 속해야 합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **Add Cluster(**클러스터 추가**)** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 지원되는 플랫폼: Firepower 9300의 FTD