Secure Firewall 3100용 클러스터링

클러스터링을 사용하면 여러 개의 FTD를 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, 39 페이지의 내용을 참조하십시오.

Secure Firewall 3100에 대한 클러스터링 정보

이 섹션에서는 클러스터링 아키텍처 및 이러한 아키텍처의 작동 방식에 대해 설명합니다.

클러스터를 네트워크에 맞게 활용하는 방법

클러스터는 하나의 유닛으로 작동하는 여러 개의 방화벽으로 구성됩니다. 클러스터로 작동하려면 방화벽에는 다음과 같은 인프라가 필요합니다.

- 클러스터 내 커뮤니케이션을 위한 분리된 고속 백플레인 네트워크(또는 클러스터 제어 링크라고 함)

- 구성 및 모니터링을 지원하는 각 방화벽에 대한 관리 액세스

네트워크에 클러스터를 배치할 경우, 업스트림 및 다운스트림 라우터에서는 스팬 EtherChannels를 사용하여 클러스터로 들어오고 나가는 데이터의 로드 밸런싱을 수행할 수 있어야 합니다. 클러스터의 여러 멤버에 대한 인터페이스는 단일 EtherChannel로 그룹화되며, EtherChannel은 유닛 간의 로드 밸런싱을 수행합니다.

제어 및 데이터 노드 역할

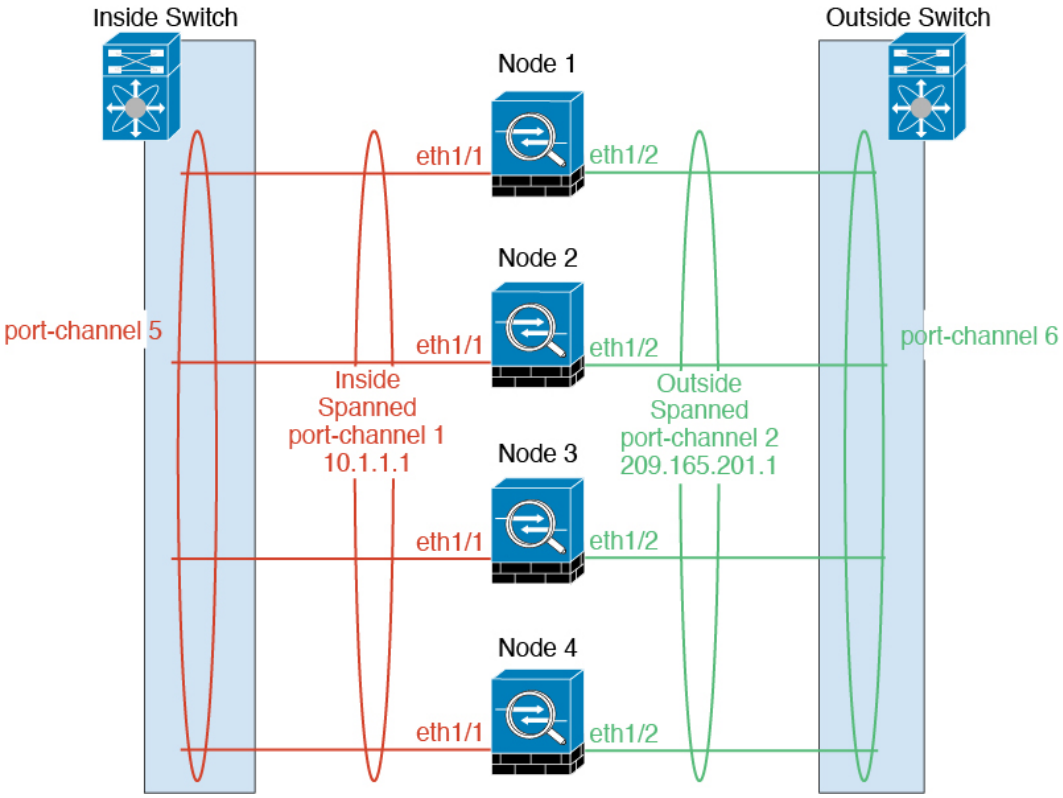
클러스터의 멤버 중 하나는 제어 노드입니다. 여러 클러스터 멤버가 동시에 온라인 상태가 되면 의 우선 순위 설정에 따라 제어 노드가 결정됩니다. 우선순위는 1에서 100까지 1이 가장 높은 우선순위입니다. 다른 모든 멤버는 데이터 노드입니다. 클러스터를 처음 생성할 때 제어 노드가 될 노드를 지정하면 클러스터에 추가된 첫 번째 노드이기 때문에 제어 노드가 됩니다.

클러스터의 모든 노드에서는 동일한 구성을 공유합니다. 처음에 제어 노드로 지정하는 노드는 클러스터에 참가할 때 데이터 노드의 구성을 덮어쓰므로 클러스터를 구성하기 전에 제어 노드에서 초기 구성만 수행하면 됩니다.

일부 기능은 클러스터로 확장되지 않으며, 제어 노드에서 이러한 기능에 대한 모든 트래픽을 처리합니다.

클러스터 인터페이스

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.



클러스터 제어 링크

각 유닛에서는 최소 1개의 하드웨어 인터페이스를 클러스터 제어 링크로 지정해야 합니다. 가능한 경우 클러스터 제어 링크에 EtherChannel을 사용하는 것이 좋습니다.

클러스터 제어 링크 트래픽 개요

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 제어 노드 선택.
- 구성 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

클러스터 제어 링크 인터페이스 및 네트워크

클러스터 제어 링크에 모든 물리적 인터페이스 또는 EtherChannel을 사용할 수 있습니다. VLAN 하위 인터페이스는 클러스터 제어 링크로 사용할 수 없습니다. 관리/진단 인터페이스도 사용할 수 없습니다.

각 클러스터 제어 링크는 동일한 서브넷에 IP 주소가 있습니다. 이 서브넷은 모든 다른 트래픽과 분리되어 있어야 하며, 클러스터 제어 링크 인터페이스만 포함해야 합니다.

참고 2-멤버 클러스터의 경우 클러스터 제어 링크를 한 노드에서 다른 노드로 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. 테스트 등을 위해 유닛을 직접 연결해야 하는 경우 클러스터를 구성하기 전에 두 노드에서 클러스터 제어 링크 인터페이스를 구성하고 활성화해야 합니다.

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.

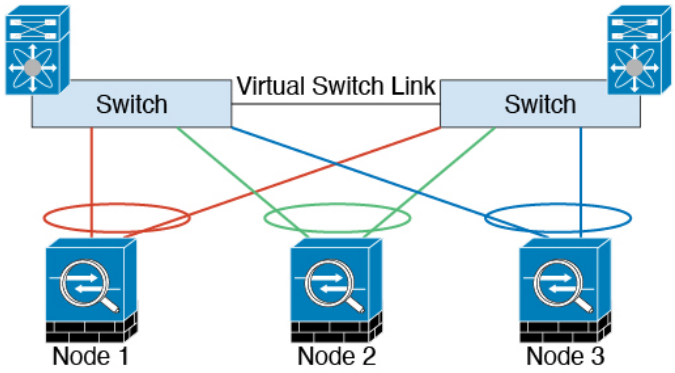
대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

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

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 단

일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스팬 EtherChannel입니다.



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.

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.

관리 네트워크

관리 인터페이스를 사용하여 각 노드를 관리해야 합니다. 데이터 인터페이스에서의 관리는 클러스터링에서 지원되지 않습니다.

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 제어 노드를 추가하는 경우 클러스터에 사용하려는 기능 라이선스를 지정할 수 있습니다. 클러스터를 생성하기 전에는 데이터 노드에 할당된 라이선스가 중요하지 않습니다. 제어 노드의 라이선스 설정은 각 데이터 노드에 복제됩니다. **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

모델 요구 사항

- Secure Firewall 3100—최대 8개 유닛

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

하드웨어 및 소프트웨어 요건

클러스터의 모든 유닛은 다음과 같아야 합니다.

- 같은 모델이어야 합니다.
- 동일한 인터페이스를 포함해야 합니다.
- FMC 액세스는 관리 인터페이스에서 이루어져야 합니다. 데이터 인터페이스 관리는 지원되지 않습니다.
- 이미지 업그레이드 시간을 제외하고는 동일한 소프트웨어를 실행해야 합니다. 무중단 업그레이드가 지원됩니다.
- 같은 방화벽 모드(라우팅 또는 투명)에 있어야 합니다.
- 동일한 도메인에 있어야 합니다.
- 동일한 그룹에 있어야 합니다.
- 보류 중이거나 진행 중인 구축이 없어야 합니다.
- 제어 노드에 지원되지 않는 기능이 구성되어서는 안 됩니다(클러스터링으로 지원되지 않는 기능, 39 페이지 참조).
- 데이터 노드에는 VPN이 구성되지 않아야 합니다. 제어 노드는 사이트 간 VPN을 구성할 수 있습니다.

스위치 요구 사항

- 클러스터링을 구성하기 전에 스위치 구성을 완료해야 합니다. 클러스터 제어 링크에 연결된 포트에 올바른(더 높은) MTU가 구성되어 있는지 확인합니다. 기본적으로 클러스터 제어 링크 MTU는 데이터 인터페이스보다 100바이트 높게 설정됩니다. 스위치에 MTU가 일치하지 않으면 클러스터 형성이 실패합니다.

클러스터링 지침

방화벽 모드

방화벽 모드는 모든 유닛과 일치해야 합니다.

고가용성

고가용성은 클러스터링에서 지원되지 않습니다.

IPv6

클러스터 제어 링크는 IPv4를 사용하는 경우에만 지원됩니다.

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.

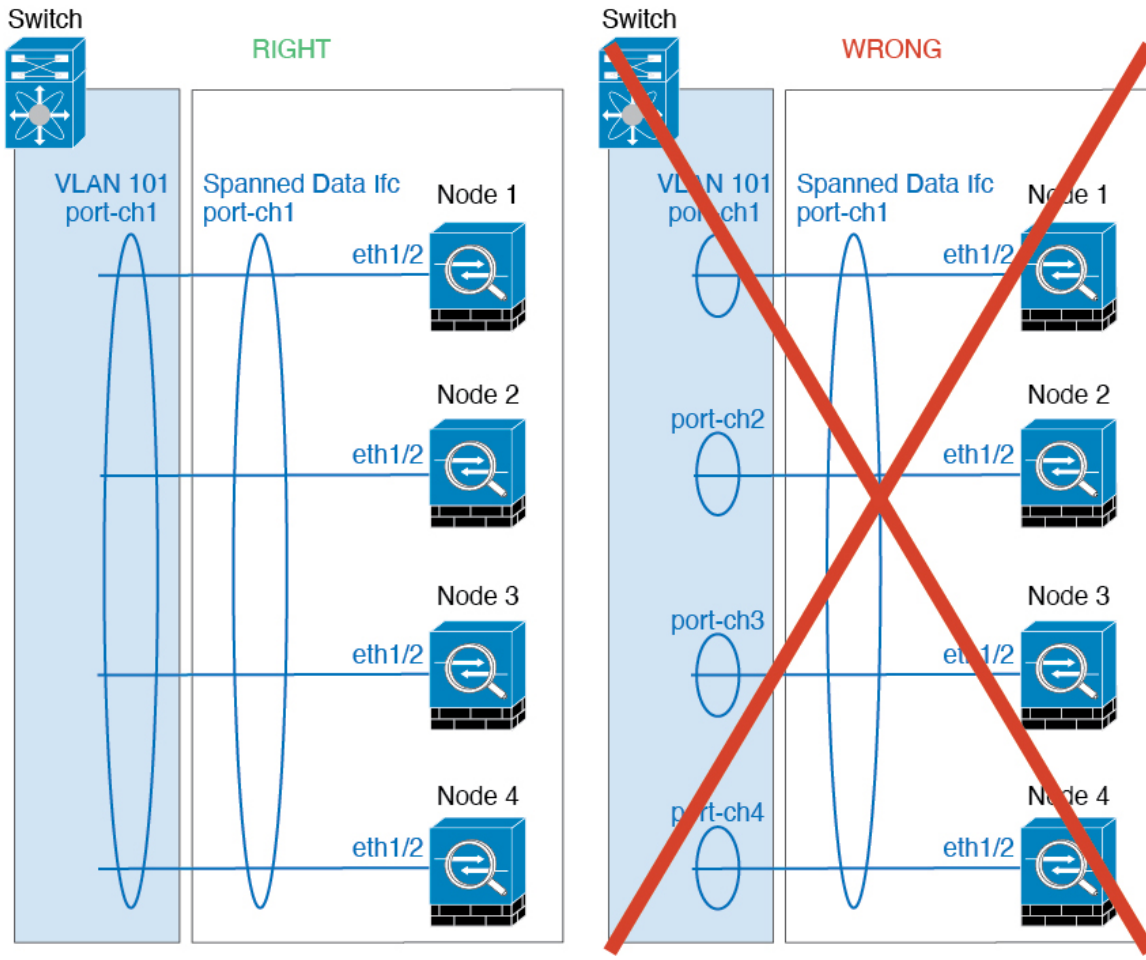
  router(config) # **port-channel** *id* **hash-distribution fixed**

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

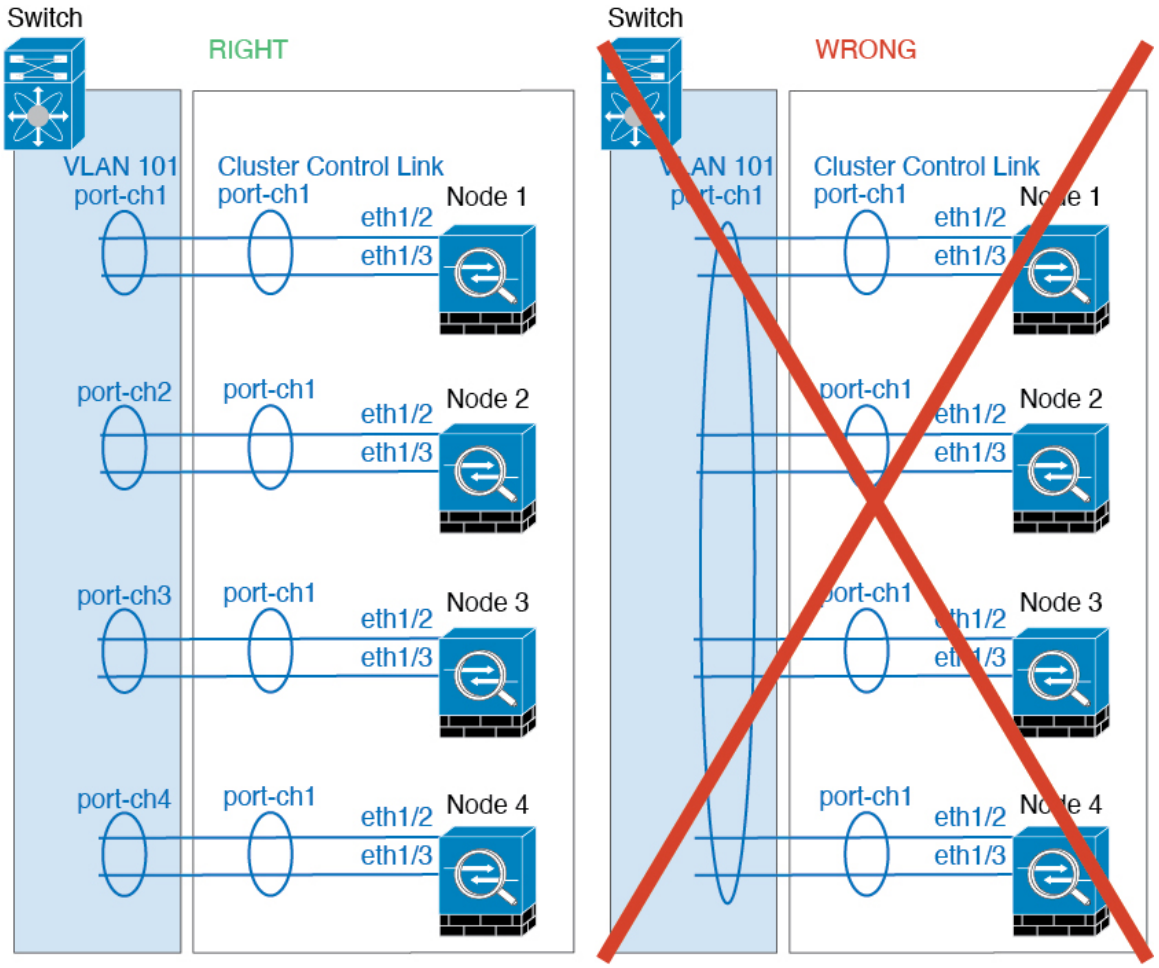
- Cisco Nexus 스위치의 경우 모든 클러스터용 EtherChannel 인터페이스에서 LACP Graceful Convergence 기능을 사용하지 않도록 설정해야 합니다.

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 EtherChannel이 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 EtherChannel에 연결된 Windows 2003 Server를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않으며, 이렇게 되면 대량의 ICMP 메시지가 ASA 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 ASA 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능이 영향을 받을 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.
- 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.

클러스터링 기본값

- cLACP 시스템 ID가 자동 생성되며 시스템 우선순위는 기본적으로 1입니다.
- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 장애가 발생한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도됩니다.
- 장애가 발생한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도됩니다.
- 5초 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

클러스터링 구성

클러스터를 FMC에 추가하려면 각 노드를 FMC에 독립형 유닛으로 추가하고 제어 노드로 만들 유닛에서 인터페이스를 구성한 다음 클러스터를 구성합니다.

FMC에 디바이스 케이블 연결 및 추가

클러스터링을 구성하기 전에 클러스터 제어 링크 네트워크, 관리 네트워크, 데이터 네트워크의 케이블을 연결합니다. FMC에서 디바이스를 독립형 유닛으로 추가합니다. 클러스터 제어 링크를 EtherChannel로 구성할 수도 있습니다.

프로시저

단계 **1** 클러스터 제어 링크 네트워크, 관리 네트워크, 데이터 네트워크의 케이블을 연결합니다.

또한 업스트림 및 다운스트림 장비도 구성해야 합니다. 스팬 EtherChannel을 케이블로 연결하는 방법에 대한 자세한 내용은 클러스터 인터페이스, 2 페이지의 내용을 참조하십시오. 클러스터 제어 링크 요구 사항은 클러스터 제어 링크 인터페이스 및 네트워크, 4 페이지의 내용을 참조하십시오.

단계 **2** 각 노드를 동일한 도메인 및 그룹에서 독립형 디바이스로 FMC에 추가합니다.

FMC에 디바이스를 추가합니다.의 내용을 참조하십시오. 단일 디바이스로 클러스터를 생성한 다음 나중에 노드를 더 추가할 수 있습니다. 디바이스를 추가할 때 설정하는 초기 설정(라이선싱, 액세스 제어 정책)은 제어 노드의 모든 클러스터 노드에 상속됩니다. 클러스터를 구성할 때 제어 노드를 선택합니다.

단계 **3** (선택 사항) 클러스터 제어 링크를 EtherChannel로 구성합니다.

a) 제어 노드가 될 디바이스에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 **Edit(**수정**)** ( )을 클릭합니다.

b) **Interfaces(**인터페이스**)**를 클릭합니다.

c) 멤버 인터페이스를 활성화합니다. 물리적 인터페이스 활성화 및 이더넷 설정 구성 섹션을 참조하십시오.

d) EtherChannel을 추가합니다. EtherChannel 구성 섹션을 참조하십시오.

클러스터 제어 링크 멤버 인터페이스에 On 모드를 사용하여 클러스터 제어 링크의 불필요한 트래픽을 줄이는 것이 좋습니다(액티브 모드가 기본값). 클러스터 제어 링크는 분리된 안정적인 네트워크이므로 LACP 트래픽의 오버헤드가 필요하지 않습니다. 참고**:** 활성 모드에 데이터 EtherChannel을 설정하는 것이 좋습니다.

클러스터 제어 링크의 이름 또는 IP 주소를 구성하지 마십시오. 이름이 없으므로 클러스터 제어 링크에 대한 MTU를 아직 설정할 수 없습니다. 클러스터를 구성한 후에는 다시 돌아와서 MTU를 설정할 수 있습니다. MTU는 데이터 인터페이스보다 100바이트 이상 높아야 합니다.

e) **Save(**저장**)**를 클릭합니다.

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

클러스터 생성

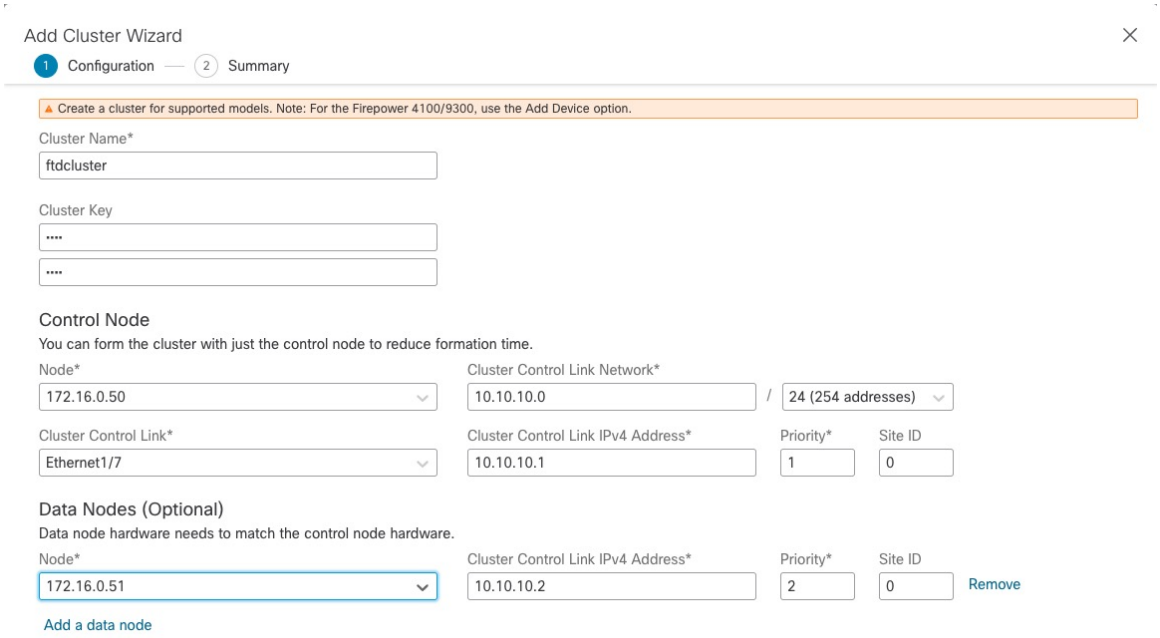
FMC에서 하나 이상의 디바이스에서 클러스터를 형성합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 **Add(**추가**)** > **Add Cluster(**클러스터 추가**)**를 선택합니다.

Add Cluster Wizard(클러스터 추가 마법사**)**가 나타납니다.

그림 *1:* 클러스터 추가 마법사



단계 **2** 제어 트래픽에 대한 클러스터 이름 및 인증 클러스터 키를 지정합니다.

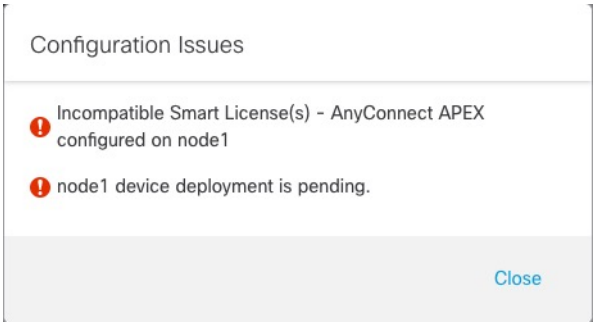
- **Cluster Name(**클러스터 이름**)**—1자 ~ 38자로 된 ASCII 문자열입니다.
- **Cluster Key(**클러스터 키**)**—1자 ~ 63자로 된 ASCII 문자열입니다. **Cluster Key(**클러스터 키**)**는 암호화 키를 생성하는 데 사용됩니다. 이 암호화는 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

단계 **3** 제어 노드에 대해 다음을 설정합니다.

- **Node(**노드**)** — 초기에 제어 노드로 사용할 디바이스를 선택합니다. FMC는 클러스터를 구성할 때 이 노드를 먼저 클러스터에 추가하므로 제어 노드가 됩니다.

참고 노드 이름 옆에 **Error(**오류**)** ( ) 아이콘이 표시되면 아이콘을 클릭하여 구성 문제를 확인합니다. 클러스터 형성을 취소하고 문제를 해결한 다음 클러스터 형성으로 돌아가야 합니다. 예를 들면 다음과 같습니다.

그림 ***2:*** 구성 문제



위의 문제를 해결하려면 지원되지 않는 VPN 라이선스를 제거하고 보류 중인 구성 변경 사항을 디바이스에 구축합니다.

- **Cluster Control Link Network(**클러스터 제어 링크 네트워크**)** - IPv4 서브넷을 지정합니다. 이 인터페이스에는 IPv6가 지원되지 않습니다. **24**, **25**, **26** 또는 **27** 서브넷을 지정합니다.
- **Cluster Control Link(**클러스터 제어 링크**)** - 클러스터 제어 링크에 사용할 물리적 인터페이스 또는 EtherChannel을 선택합니다.
- **Cluster Control Link IPv4 Address(**클러스터 제어 링크 **IPv4** 주소**)** - 이 필드는 클러스터 제어 링크 네트워크의 첫 번째 주소로 자동 채워집니다. 원하는 경우 호스트 주소를 편집할 수 있습니다.
- **Priority(**우선순위**)** — 제어 노드 선택을 위해 이 노드의 우선순위를 설정합니다. 우선순위는 1에서 100까지이며 1이 가장 높은 우선순위입니다. 우선순위를 다른 노드보다 낮게 설정한 경우에도 클러스터가 처음 구성될 때 이 노드는 여전히 제어 노드가 됩니다.
- **Site ID(**사이트 **ID)** — (FlexConfig 기능) 이 노드의 사이트 ID를 1~8 사이로 입력합니다. 값이 0이면 사이트 간 클러스터링이 비활성화됩니다. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.

단계 **4** **Data Nodes (Optional)(**데이터 노드**(**선택 사항**))**에서 **Add a data node(**데이터 노드 추가**)**를 클릭하여 클러스터에 노드를 추가합니다.

더 빠른 클러스터 형성을 위해 제어 노드만 사용하여 클러스터를 형성하거나 모든 노드를 지금 추가할 수 있습니다. 각 데이터 노드에 대해 다음을 설정합니다.

- **Node(**노드**)** — 추가할 디바이스를 선택합니다.

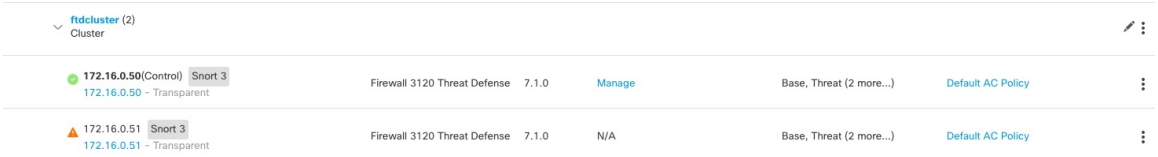
참고 노드 이름 옆에 **Error(**오류**)** ( ) 아이콘이 표시되면 아이콘을 클릭하여 구성 문제를 확인합니다. 클러스터 형성을 취소하고 문제를 해결한 다음 클러스터 형성으로 돌아가야 합니다.

- **Cluster Control Link IPv4 Address(**클러스터 제어 링크 **IPv4** 주소**)** - 이 필드는 클러스터 제어 링크 네트워크의 다음 주소로 자동 채워집니다. 원하는 경우 호스트 주소를 편집할 수 있습니다.
- **Priority(**우선순위**)** — 제어 노드 선택을 위해 이 노드의 우선순위를 설정합니다. 우선순위는 1에서 100까지이며 1이 가장 높은 우선순위입니다.
- **Site ID(**사이트 **ID)** — (FlexConfig 기능) 이 노드의 사이트 ID를 1~8 사이로 입력합니다. 값이 0이면 사이트 간 클러스터링이 비활성화됩니다. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.

단계 **5** **Continue(**계속**)**를 클릭합니다. **Summary(**요약**)**를 검토하고 **Save(**저장**)**를 클릭합니다.

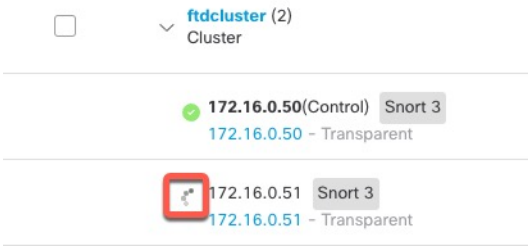
디바이스 > 디바이스 관리 페이지에 클러스터 이름이 표시됩니다. 클러스터 노드를 보려면 클러스터를 확장합니다.

그림 ***3:*** 클러스터 관리

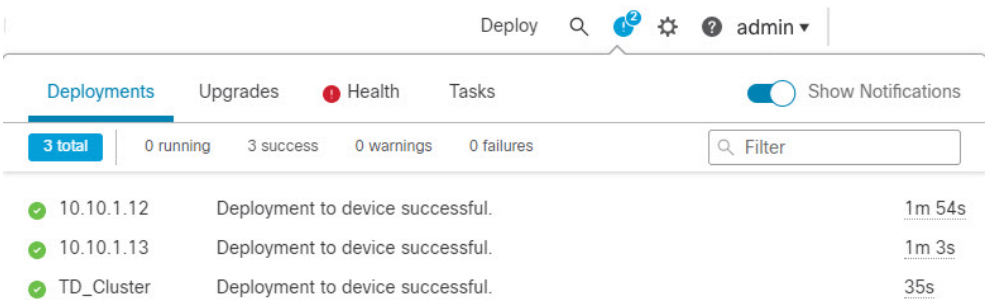


현재 등록되는 노드에는 로딩 아이콘이 표시됩니다.

그림 ***4:*** 노드 등록



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 노드 등록을 모니터링할 수 있습니다. FMC은 각 노드가 등록될 때마다 클러스터 등록 작업을 업데이트합니다.

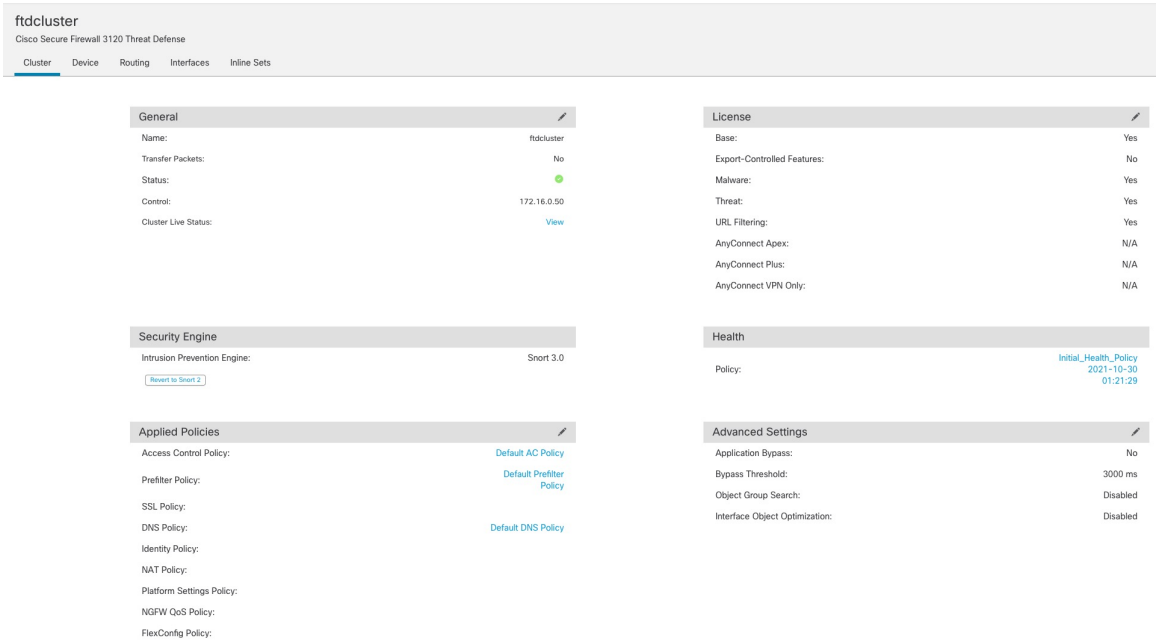


단계 **6** 클러스터에 대해 **Edit(**수정**)** ( )을 클릭하여 디바이스별 설정을 구성합니다.

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

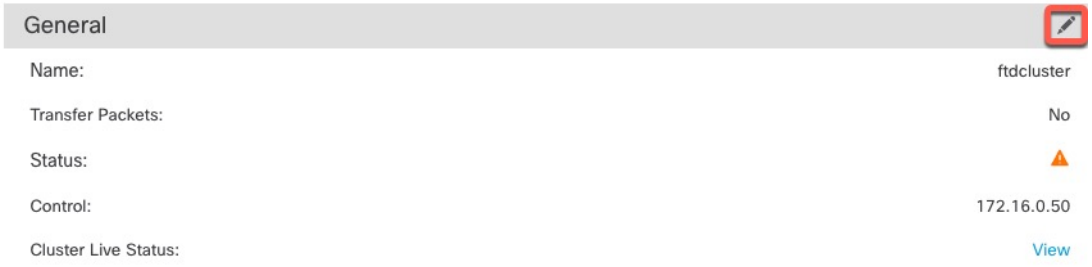
단계 **7** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 화면에서 **General(**일반**)** 및 클러스터에 대한 기타 설정을 표시합니다.

그림 *5:* 클러스터 설정

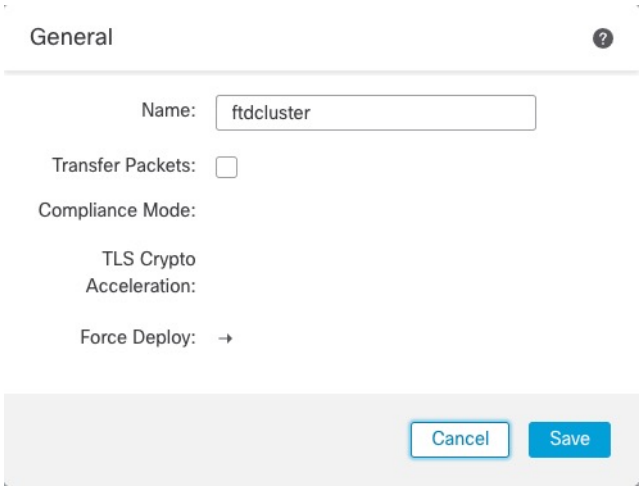


General(일반**)** 영역에서 다음 클러스터별 항목을 참조하십시오.

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

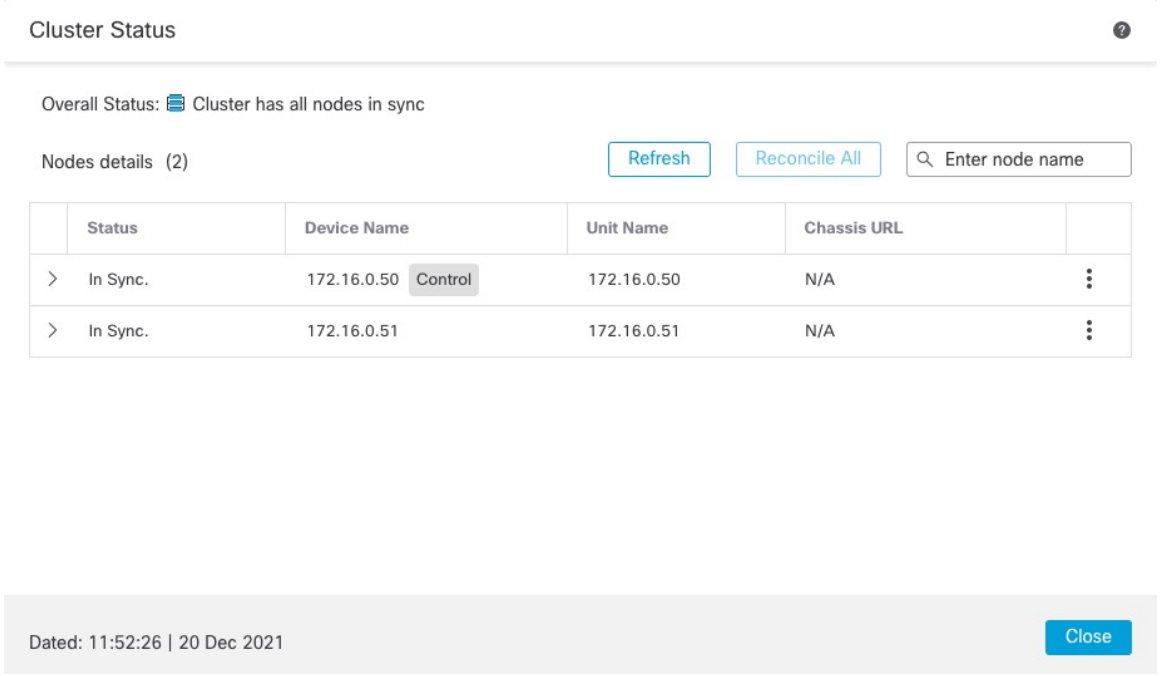


그런 다음 **Name(**이름**)** 필드를 설정합니다.



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

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



단계 **8** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 디바이스**(**디바이스**)**의 오른쪽 상단 드롭다운 메뉴에서 클러스터의 각 멤버를 선택하고 다음 설정을 구성할 수 있습니다.

그림 ***6:*** 디바이스 설정

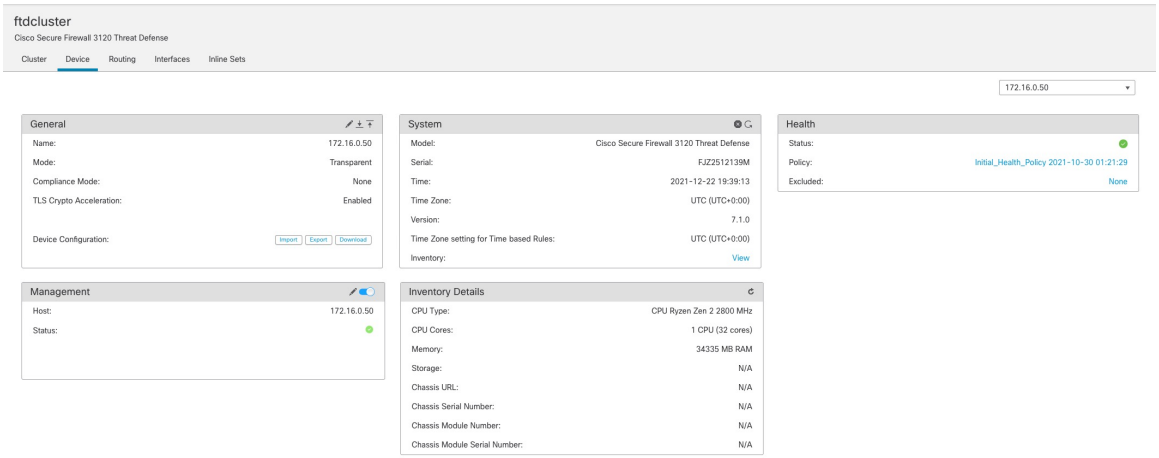
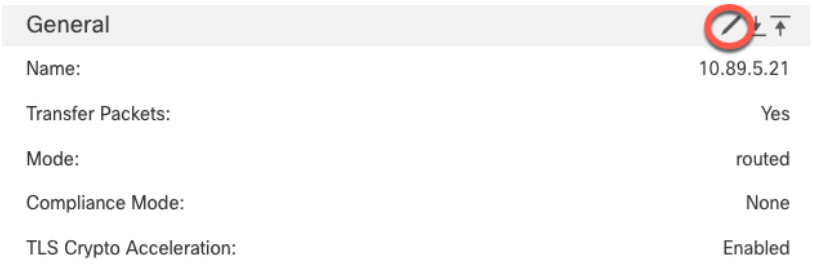
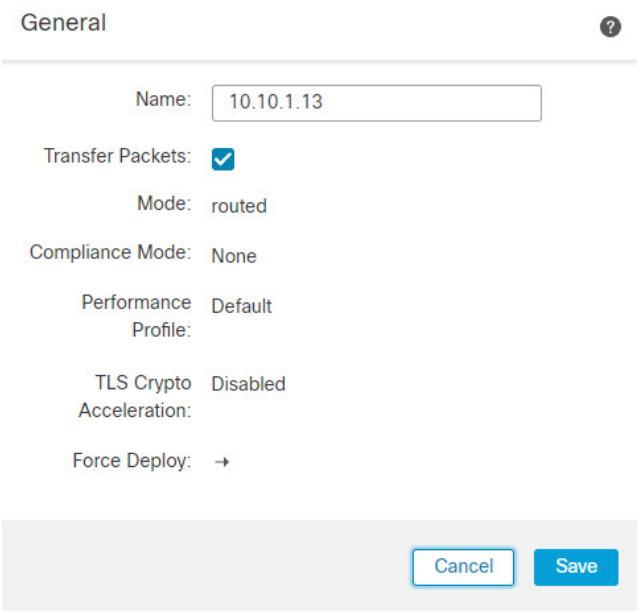


그림 ***7:*** 노드 선택

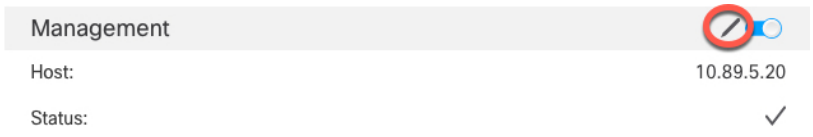
- **General(**일반**)** > **Name (**이름**)** - **Edit(**수정**)** ( )을 클릭하여 클러스터 멤버 표시 이름을 변경합니다.



그런 다음 **Name(**이름**)** 필드를 설정합니다.



- **Management(**관리**) > Host(**호스트**)**—디바이스 구성에서 관리 IP 주소를 변경하는 경우 새 주소를 FMC에 일치시켜야 네트워크의 디바이스와 연결할 수 있습니다. 먼저 연결을 비활성화하고 **Management(**관리**)** 영역에서 **Host(**호스트**)** 주소를 편집한 다음 연결을 다시 활성화합니다.



인터페이스 구성

데이터 인터페이스를 스팬 EtherChannel로 구성합니다. 클러스터 제어 링크 인터페이스의 경우 MTU를 기본값에서 늘려야 합니다. 개별 인터페이스로 실행할 수 있는 유일한 인터페이스인 진단 인터페이스를 구성할 수도 있습니다.

프로시저

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

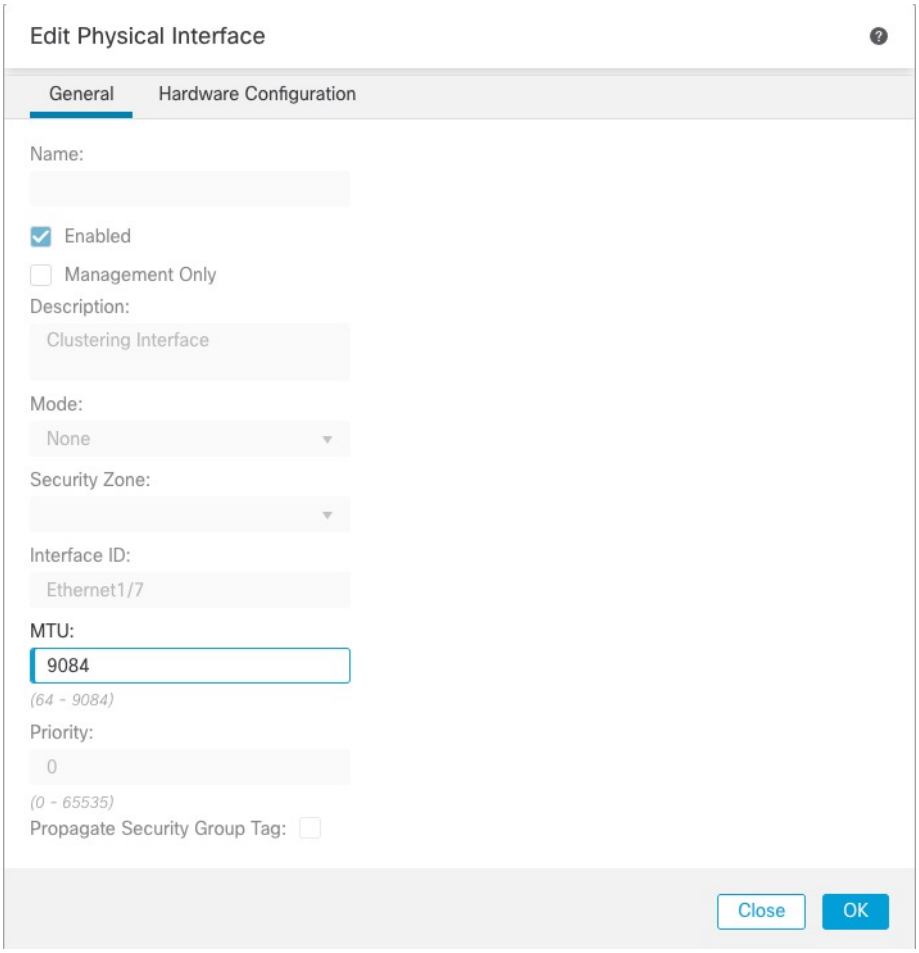
단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

단계 **3** 클러스터 제어 링크 IP 네트워크를 설정합니다.

a) 클러스터 제어 링크 인터페이스에 대한 **Edit(**수정**)** ( )를 클릭합니다.

b) **General(**일반**)** 페이지의 **MTU** 필드에 1400바이트 이상의 값을 입력합니다. 최대 MTU를 사용하는 것이 좋습니다.

그림 ***8: MTU*** 설정



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 최대값으로 설정하는 것이 좋습니다. 최소값은 1400바이트입니다. 예를 들어 최대 MTU가 9084바이트이므로 가장 높은 데이터 인터페이스 MTU는 8984가 될 수 있는 반면, 클러스터 제어 링크는 9084로 설정할 수 있습니다.

참고 클러스터 제어 링크에 연결된 스위치를 올바른 (상위) MTU로 구성해야 합니다. 그렇지 않으면 클러스터 형성이 실패합니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** 스팬 EtherChannel 데이터 인터페이스를 구성합니다.

a) EtherChannel을 하나 이상 구성합니다. EtherChannel 구성의 내용을 참조하십시오.

EtherChannel에 하나 이상의 멤버 인터페이스를 포함할 수 있습니다. 이 EtherChannel은 모든 노드에 걸쳐 있으므로 노드당 하나의 멤버 인터페이스만 있으면 됩니다. 그러나 처리량과 이중화를 높이려면 여러 멤버를 사용하는 것이 좋습니다.

b) (선택 사항) EtherChannel에 VLAN 하위 인터페이스를 구성합니다. 이 절차의 나머지는 하위 인터페이스에 적용됩니다. 하위 인터페이스 추가를 참조하십시오.

c) EtherChannel 인터페이스에 대해 **Edit(**수정**)** (✎)을 클릭합니다.

d) 라우팅 모드 인터페이스 구성 또는 투명 모드의 경우 브리지 그룹 인터페이스 구성에 따라 이름, IP 주소 및 기타 매개변수를 구성합니다.

참고 클러스터 제어 링크 인터페이스 MTU가 데이터 인터페이스 MTU보다 최소 100바이트 이상 높지 않으면 데이터 인터페이스의 MTU를 줄여야 한다는 오류가 표시됩니다.

e) 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.

f) **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.

클러스터 노드 관리

클러스터를 배치한 후에는 구성을 변경하고 클러스터 노드를 관리할 수 있습니다.

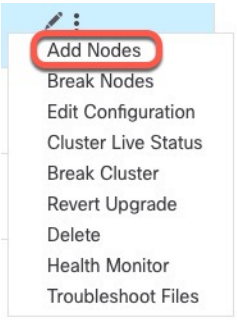
새 클러스터 노드 추가

기존 클러스터에 하나 이상의 새 클러스터 노드를 추가할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 클러스터에 대해 추가 ( )를 클릭하고 **Add Nodes(**노드 추가**)**를 선택합니다.

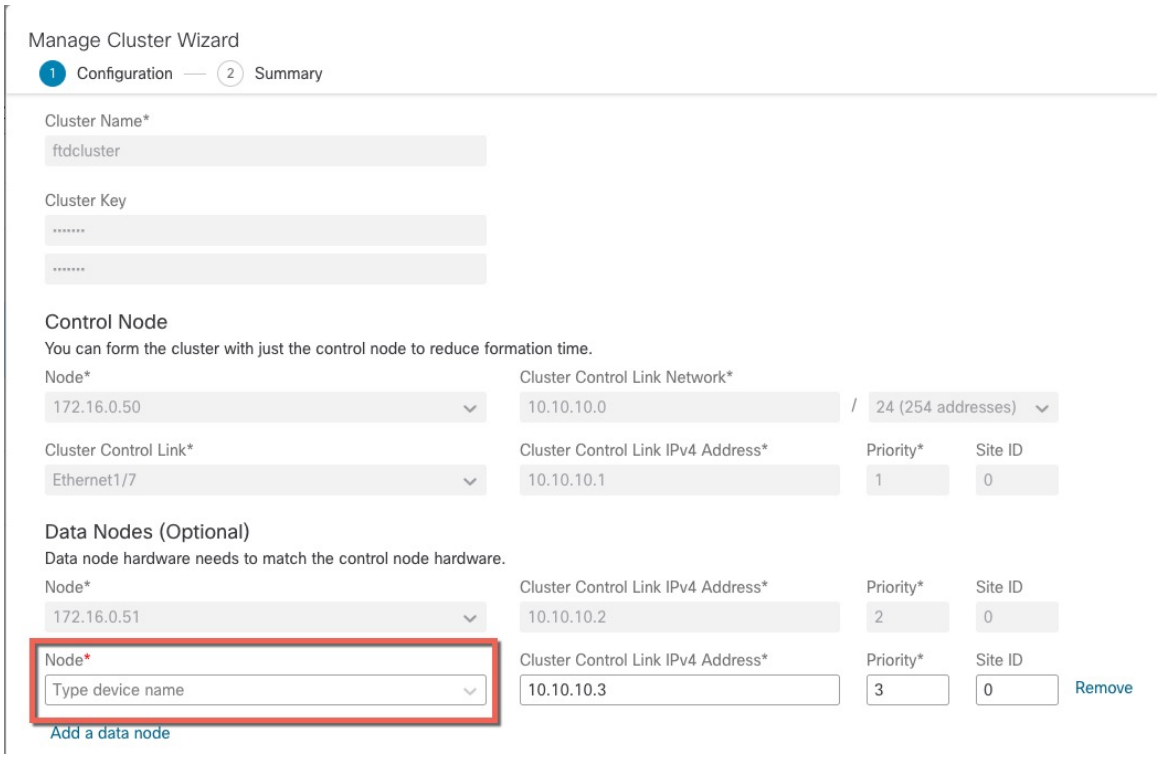
그림 ***9:*** 노드 추가



Manage Cluster Wizard(클러스터 관리 마법사**)**가 나타납니다.

단계 **2** **Node(**노드**)** 메뉴에서 디바이스를 선택하고 원하는 경우 IP 주소, 우선순위 및 Site ID(사이트 ID)를 조정합니다.

그림 *10:* 클러스터 마법사 관리



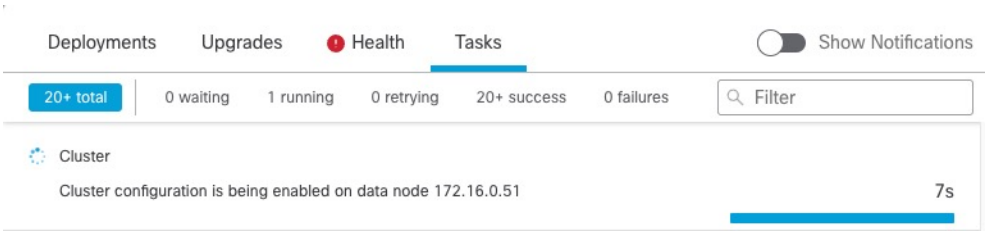
단계 **3** 노드를 추가하려면 **Add data node(**데이터 노드 추가**)**를 클릭합니다.

단계 **4** **Continue(**계속**)**를 클릭합니다. **Summary(**요약**)**를 검토하고 **Save(**저장**)**를 클릭합니다.

현재 등록되는 노드에는 로딩 아이콘이 표시됩니다.

그림 *11:* 노드 등록

알림 아이콘을 클릭하고 작업을 선택하여 클러스터 노드 등록을 모니터링할 수 있습니다.



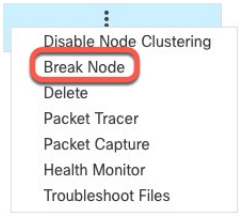
노드 분리

클러스터에서 노드를 제거하여 독립형 디바이스가 되도록 할 수 있습니다. 전체 클러스터를 분리하지 않는 한 제어 노드를 분리할 수 없습니다. 데이터 노드의 구성이 지워졌습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 분리할 노드의 추가 (⋮)을 클릭한 다음 **Break Node(**노드 분리**)**를 선택합니다.

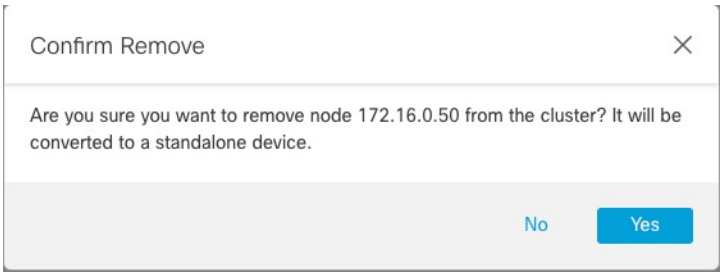
그림 ***12:*** 노드 분리



Break Nodes(노드 분리**)**를 선택하여 클러스터 More(추가) 메뉴에서 하나 이상의 노드를 분리할 수 있습니다.

단계 **2** 중단을 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***13:*** 분리 확인



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 노드 분리를 모니터링할 수 있습니다.

클러스터 분리

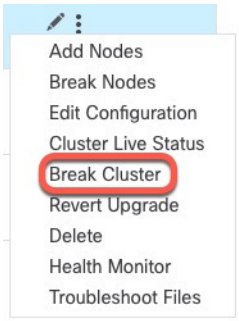
클러스터를 분리하고 모든 노드를 독립형 디바이스로 변환할 수 있습니다. 제어 노드는 인터페이스 및 보안 정책 구성을 유지하는 반면, 데이터 노드는 해당 구성을 지웁니다.

프로시저

단계 **1** 노드를 조정하여 모든 클러스터 노드가 FMC에서 관리되고 있는지 확인합니다. 클러스터 노드 조정, 29 페이지의 내용을 참조하십시오.

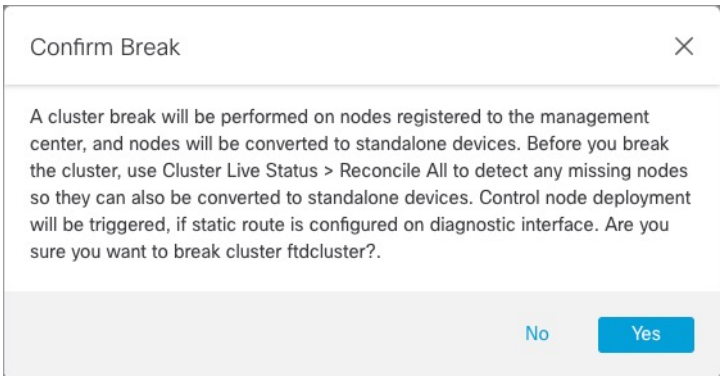
단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 클러스터에 대해 추가 (⋮)를 클릭하고 **Break Cluster(**클러스터 분리**)**를 선택합니다.

그림 ***14:*** 클러스터 분리



단계 **3** 클러스터를 분리하라는 프롬프트가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***15:*** 분리 확인



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 분리를 모니터링할 수 있습니다.

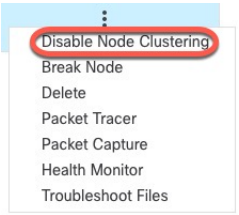
클러스터링 비활성화

노드 삭제를 준비하거나 유지 보수를 위해 일시적으로 노드를 비활성화할 수 있습니다. 이 절차는 노드를 일시적으로 비활성화하기 위함이며, FMC 디바이스 목록에 노드를 유지해야 합니다. 노드가 비활성 상태가 되면 모든 데이터 인터페이스가 종료됩니다.

프로시저

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

그림 ***16:*** 클러스터링 비활성화



제어 노드에서 클러스터링을 비활성화하면 데이터 노드 중 하나가 새 제어 노드가 됩니다. 중앙 집중식 기능의 경우 제어 노드를 강제로 변경하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다. 클러스터의 유일한 노드인 경우 제어 노드에서 클러스터링을 비활성화할 수 없습니다.

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

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

단계 **3** 클러스터링을 다시 활성화하려면 클러스터 재참가, 26 페이지의 내용을 참조하십시오.

클러스터 재참가

예를 들어 인터페이스 오류 등으로 노드가 클러스터에서 제거되거나 수동으로 클러스터링을 비활성화한 경우 클러스터를 수동으로 다시 참가시킬 수 있습니다. 클러스터 다시 조인을 시도하기 전에 오류가 해결되었는지 확인하십시오. 노드가 클러스터에서 제거되는 이유에 대한 자세한 내용은 클러스터 다시 참가, 46 페이지의 내용을 참조하십시오.

프로시저

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

단계 **2** 유닛에서 클러스터링을 활성화할지 확인합니다.

제어 노드 변경

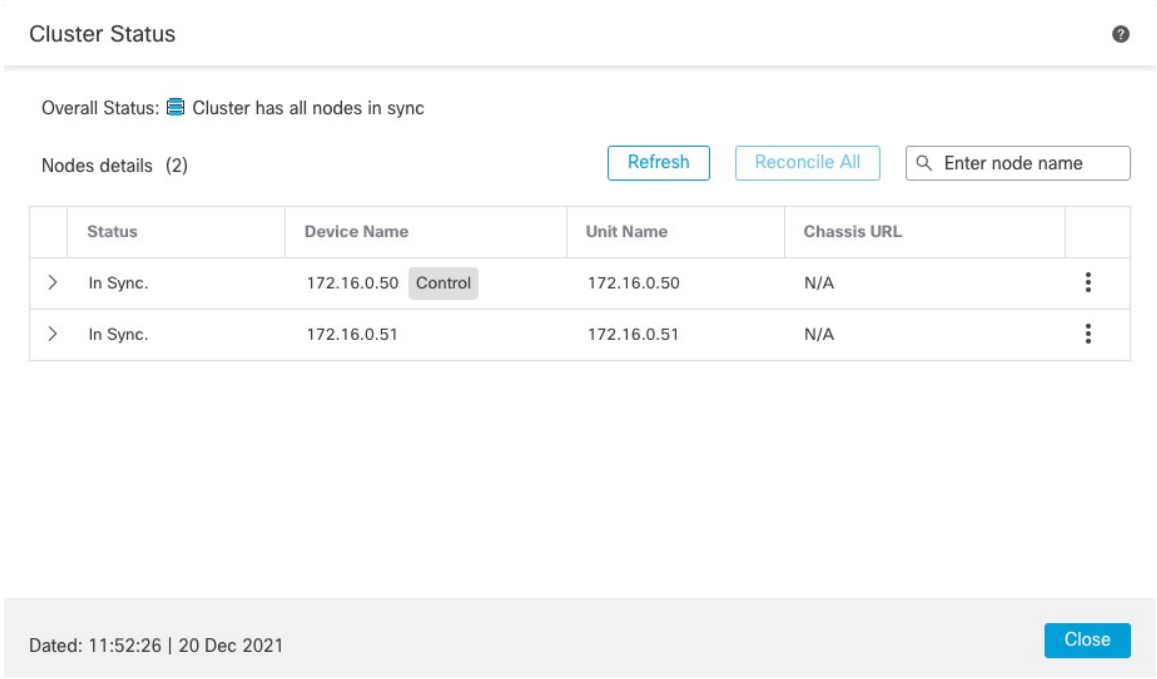
주의 제어 노드를 변경하는 가장 좋은 방법은 제어 노드의 클러스터링을 비활성화한 후 새 제어가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 제어 노드가 될 정확한 유닛을 지정해야 할 경우, 이 섹션의 절차를 참조하십시오. 중앙 집중식 기능의 경우 두 가지 방법을 사용하여 제어 노드를 강제로 변경하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다.

제어 노드를 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.

그림 ***17:*** 클러스터 상태



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.

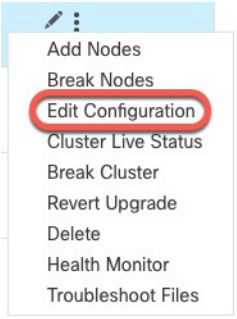
클러스터 구성 편집

클러스터 구성을 편집할 수 있습니다. 클러스터 키, 클러스터 제어 링크 인터페이스 또는 클러스터 제어 링크 네트워크를 변경하면 클러스터가 자동으로 중단되고 다시 구성됩니다. 클러스터를 재구성할 때까지 트래픽 중단이 발생할 수 있습니다. 노드, 노드 우선순위 또는 사이트 ID에 대한 클러스터 제어 링크 IP 주소를 변경하면 영향을 받는 노드만 중단되고 클러스터에 추가됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 클러스터에 대해 추가 ( )를 클릭하고 **Edit Configuration(**구성 편집**)**을 선택합니다.

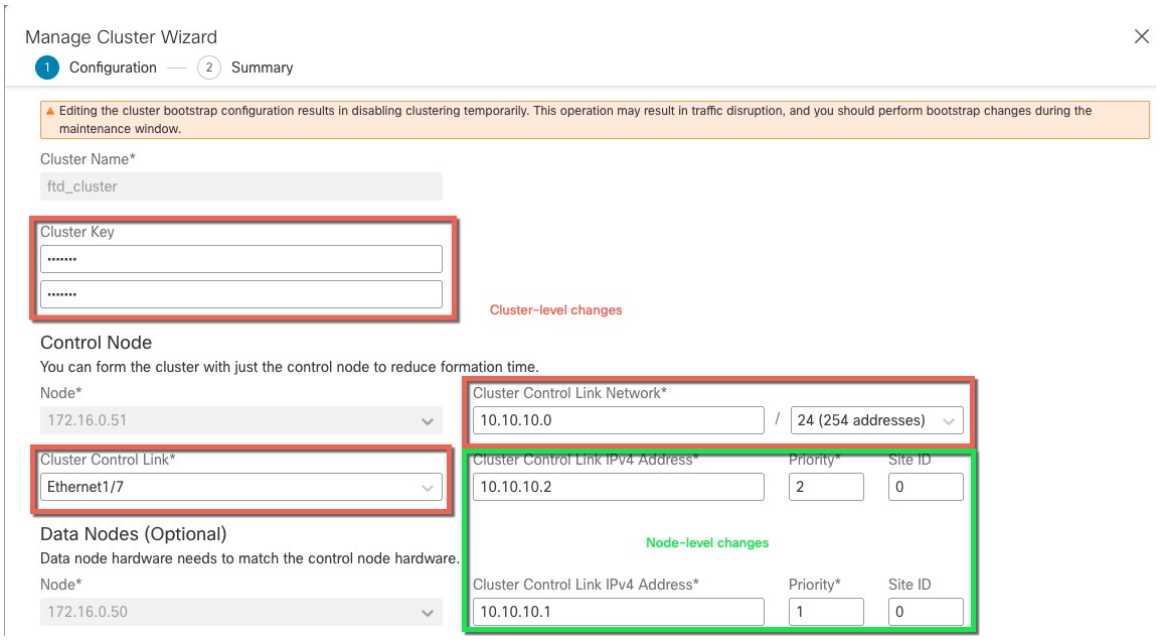
그림 ***18:*** 구성 편집



Manage Cluster Wizard(클러스터 관리 마법사**)**가 나타납니다.

단계 **2** 클러스터 구성을 업데이트합니다.

그림 *19:* 클러스터 마법사 관리



클러스터 제어 링크가 EtherChannel인 경우 인터페이스 드롭다운 메뉴 옆에 있는 **Edit(**수정**)** ( )을 클릭하여 인터페이스 멤버십 및 LACP 구성을 편집할 수 있습니다.

단계 **3** **Continue(**계속**)**를 클릭합니다. **Summary(**요약**)**를 검토하고 **Save(**저장**)**를 클릭합니다.

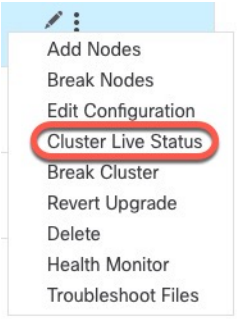
클러스터 노드 조정

클러스터 노드 등록에 실패하면 디바이스에서 FMC에 대해 클러스터 멤버십을 다시 조정합니다. 예를 들어, FMC이 특정 프로세스 중이거나 네트워크에 문제가 있는 경우, 데이터 노드 등록에 실패할 수 있습니다.

프로시저

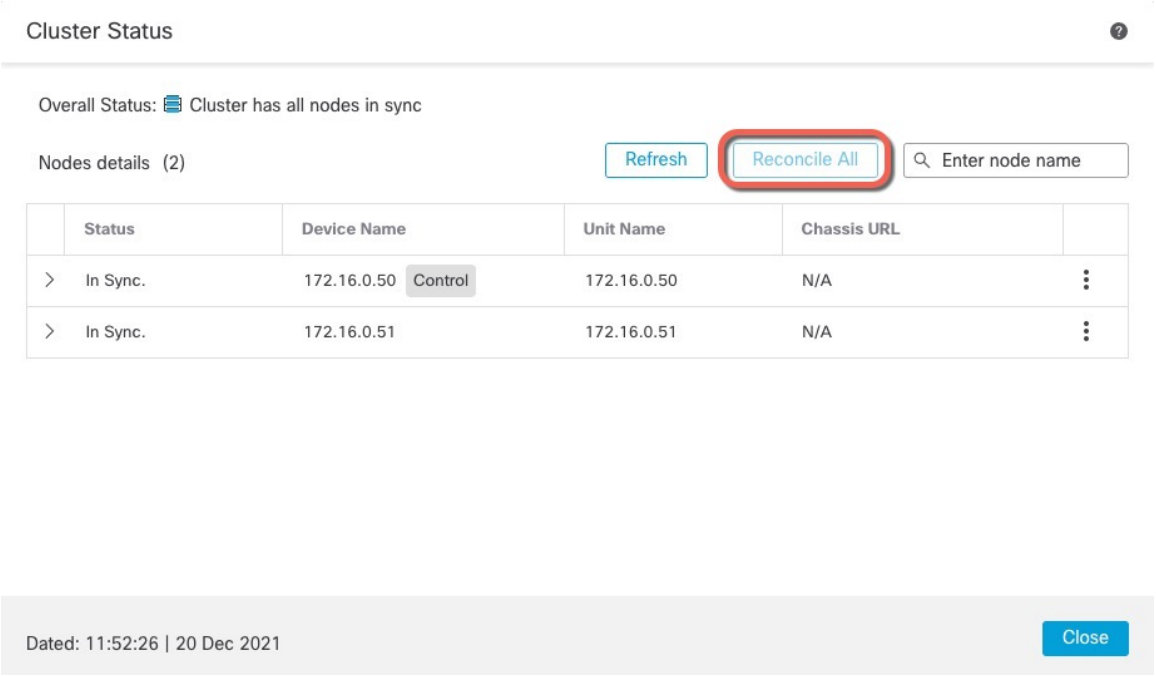
단계 **1** 클러스터에 대해 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 추가 ( )를 선택한 다음 **Cluster Live Status(**클러스터 라이브 상태**)**를 선택하여 **Cluster Status(**클러스터 상태**)** 대화 상자를 엽니다.

그림 *20:* 클러스터 라이브 상태



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

그림 *21:* 모두 조정



클러스터 상대에 대한 자세한 내용은 클러스터 모니터링, 31 페이지을 참고하십시오.

Management Center에서 클러스터 또는 노드 삭제

FMC에서 클러스터를 삭제할 수 있습니다. 그러면 클러스터는 그대로 유지됩니다. 클러스터를 새 FMC에 추가하려는 경우 클러스터를 삭제할 수 있습니다.

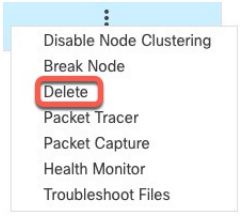
클러스터에서 노드를 분리하지 않고 FMC에서 노드를 삭제할 수도 있습니다. 노드는 FMC에 표시되지 않지만 여전히 클러스터의 일부이며 트래픽을 계속 전달하며 제어 노드가 될 수도 있습니다. 현재

제어 노드는 삭제할 수 없습니다. FMC에서 노드에 더 이상 연결할 수 없지만 클러스터의 일부로 유지하려는 경우 노드를 삭제할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 클러스터 또는 노드로 추가 ( ) 를 클릭하고 **Delete(**삭제**)**를 선택합니다.

그림 ***22:*** 클러스터 또는 노드 삭제



단계 **2** 클러스터 또는 노드를 삭제하라는 프롬프트가 표시됩니다. **Yes(**예**)**를 클릭합니다.

단계 **3** 클러스터를 새 FMC에 추가하려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택한 다음 **Add Device(**디바이스 추가**)**를 클릭합니다.

클러스터 멤버 중 하나만 디바이스로 추가하면 나머지 클러스터 노드가 검색됩니다.

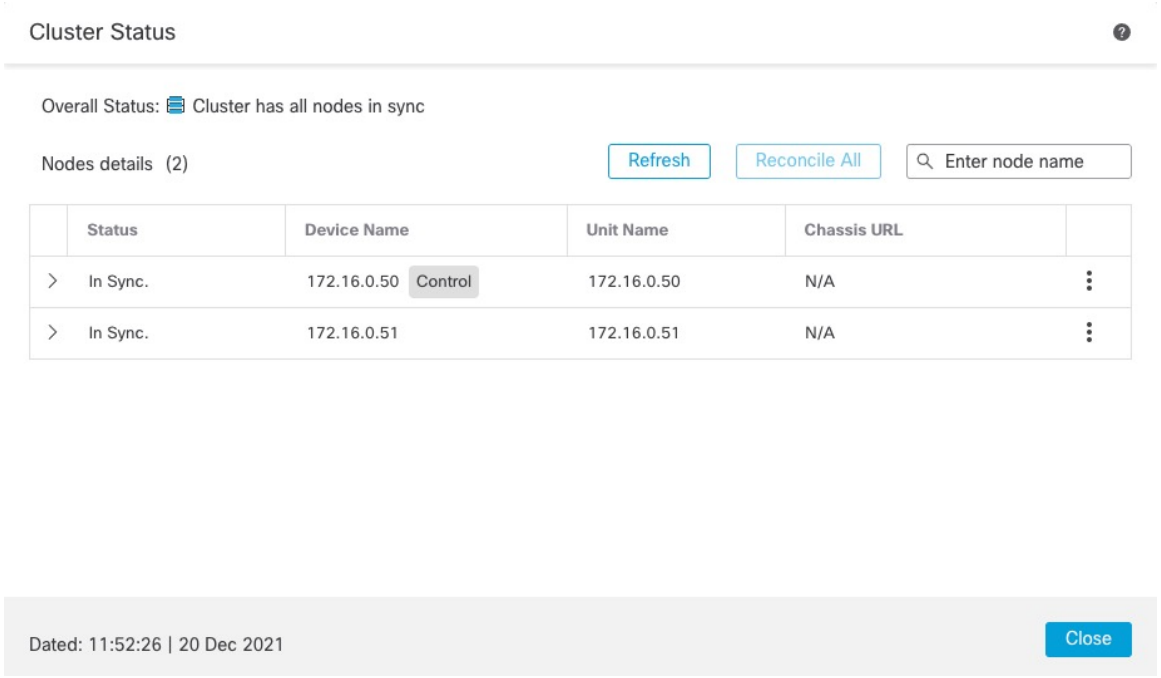
삭제된 노드를 다시 추가하려면 클러스터 노드 조정, 29 페이지의 내용을 참조하십시오.

클러스터 모니터링

FMC과 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**)** 링크에서 제공됩니다.

그림 ***23:*** 클러스터 상태



제어 노드에는 역할을 식별하는 그래픽 표시기가 있습니다.

클러스터 멤버 상태에는 다음 상태가 포함됩니다.

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

각 노드에 대해 요약 또는 기록을 볼 수 있습니다.

그림 ***24:*** 노드 요약

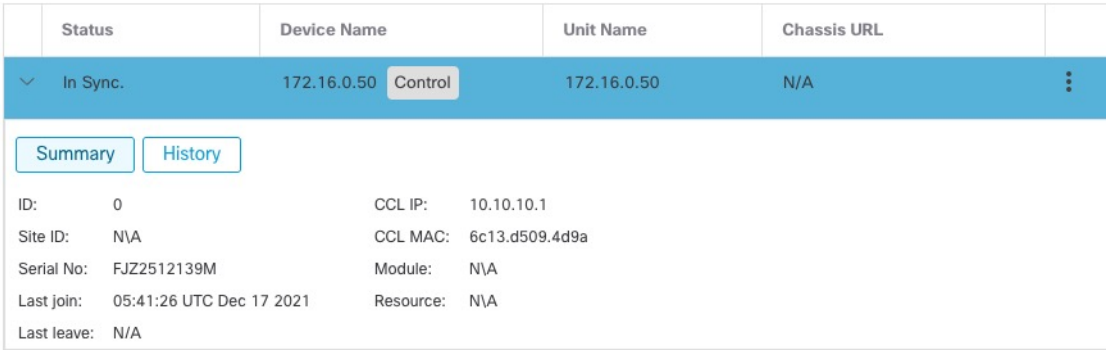
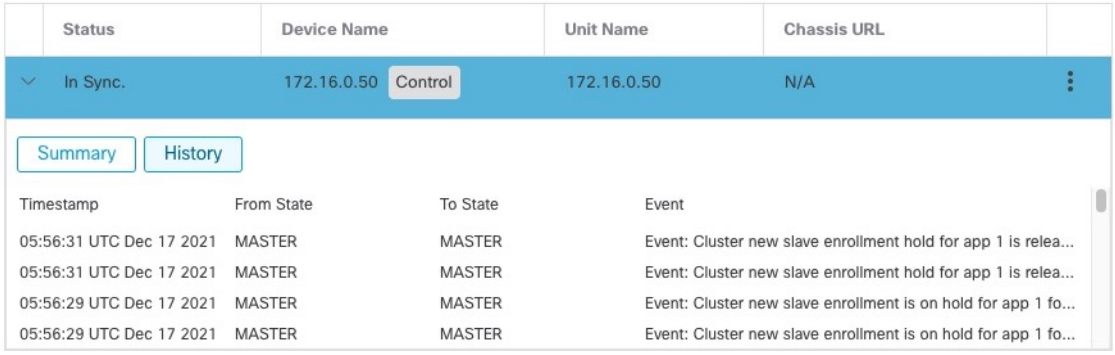


그림 ***25:*** 노드 기록



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

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

- **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > *cluster_name*.

  디바이스 목록 페이지에서 클러스터를 확장하는 경우, IP 주소 옆에 해당 역할과 함께 표시되는 제어 노드를 포함하여 모든 멤버 노드를 볼 수 있습니다. 아직 등록 중인 로드는 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.

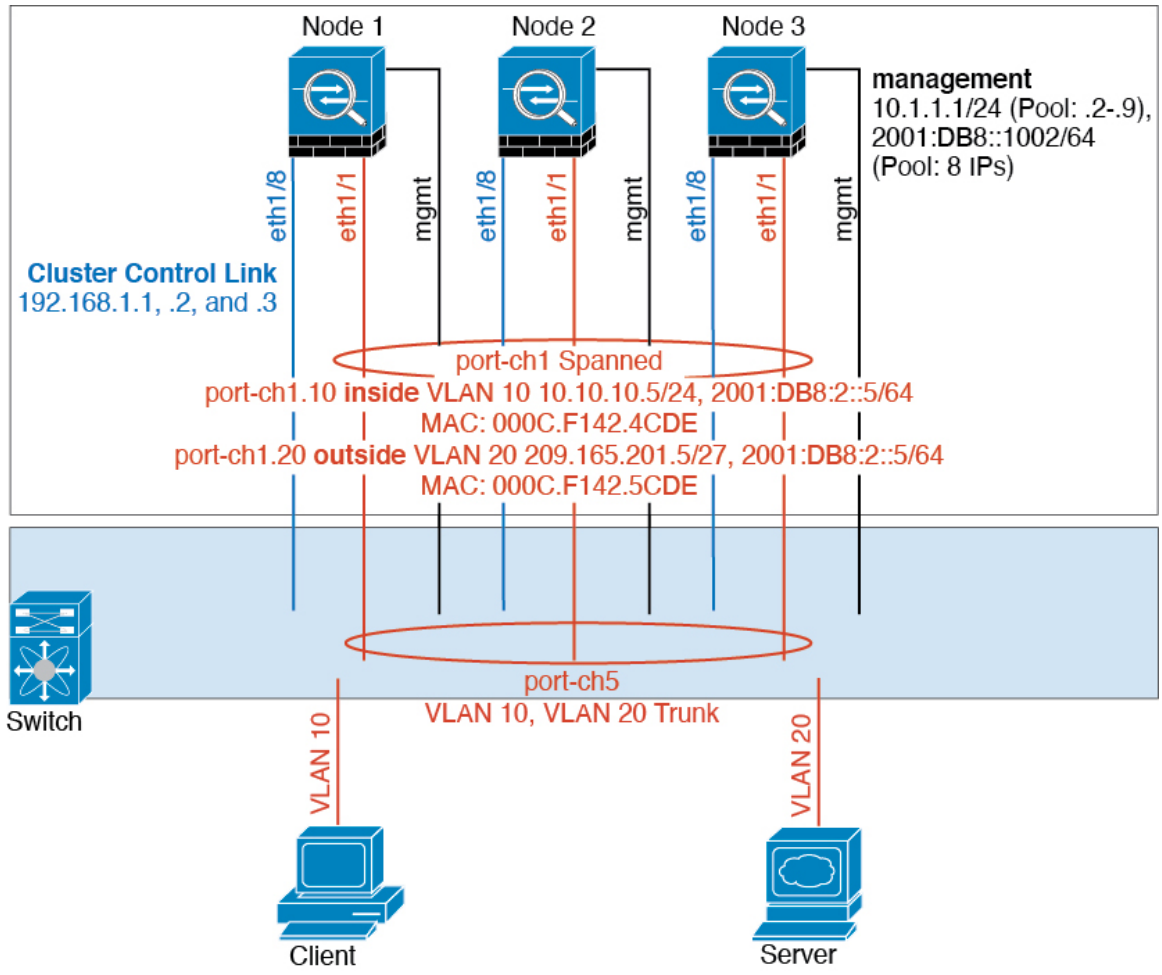
- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

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

클러스터링의 예

이러한 예에는 일반적인 구축에 대한 예가 포함되어 있습니다.

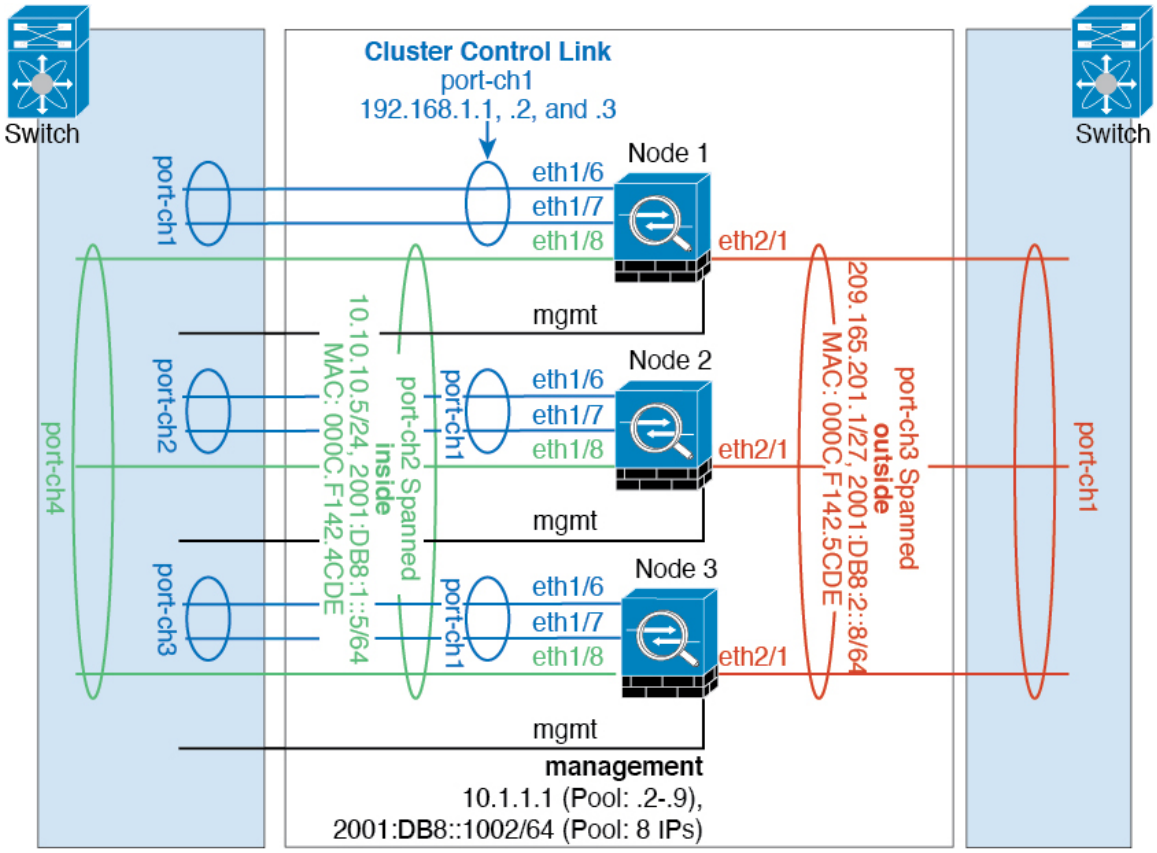
단일화된 방화벽



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

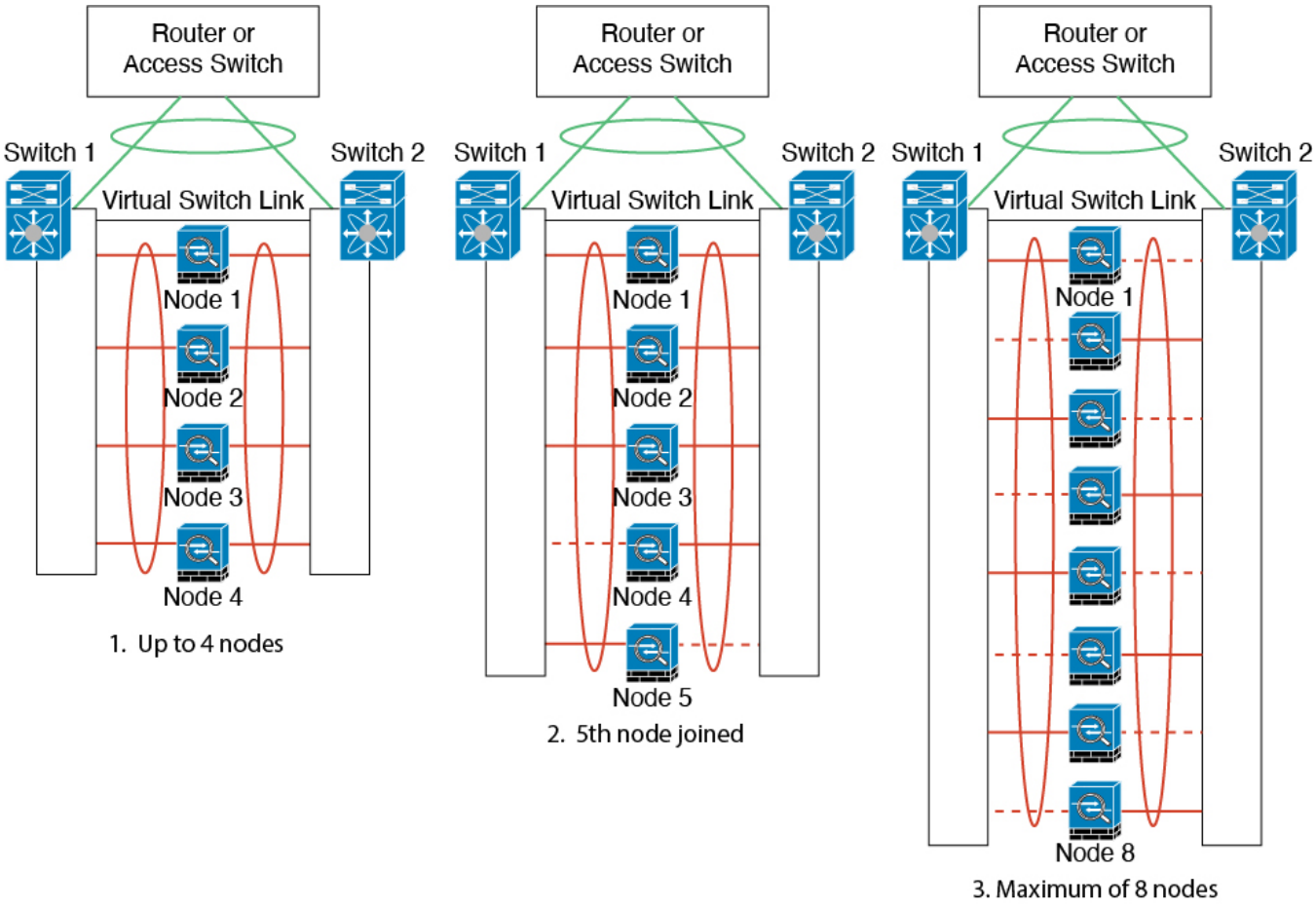


내부 네트워크와 외부 네트워크 간의 트래픽을 물리적으로 분리하려는 경우가 있습니다.

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.

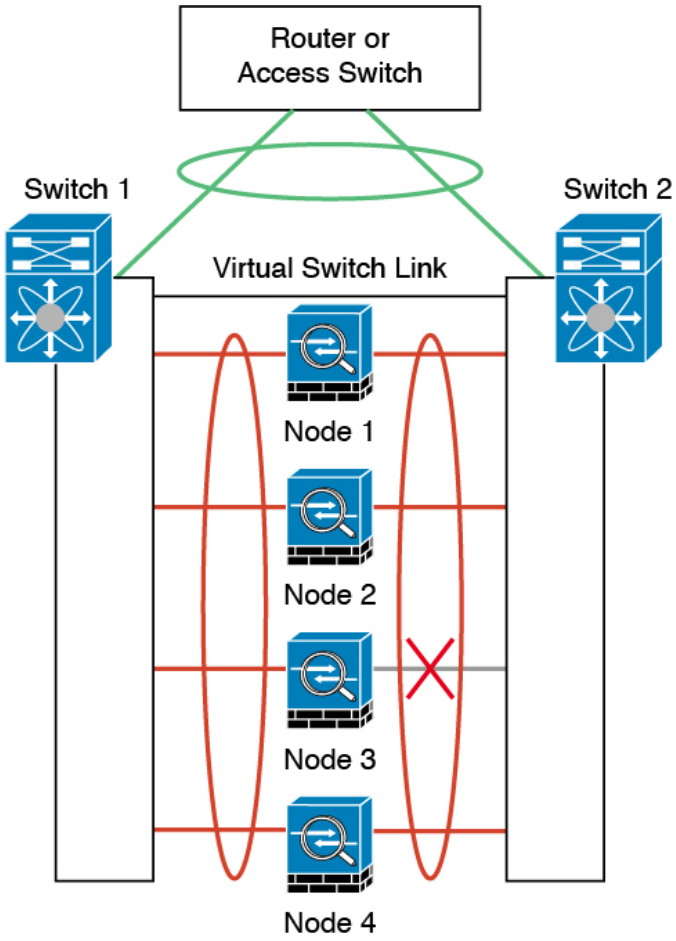
백업 링크가 포함된 스팬 **EtherChannel**(기존 **8** 액티브 포트**/8** 스탠바이)

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.

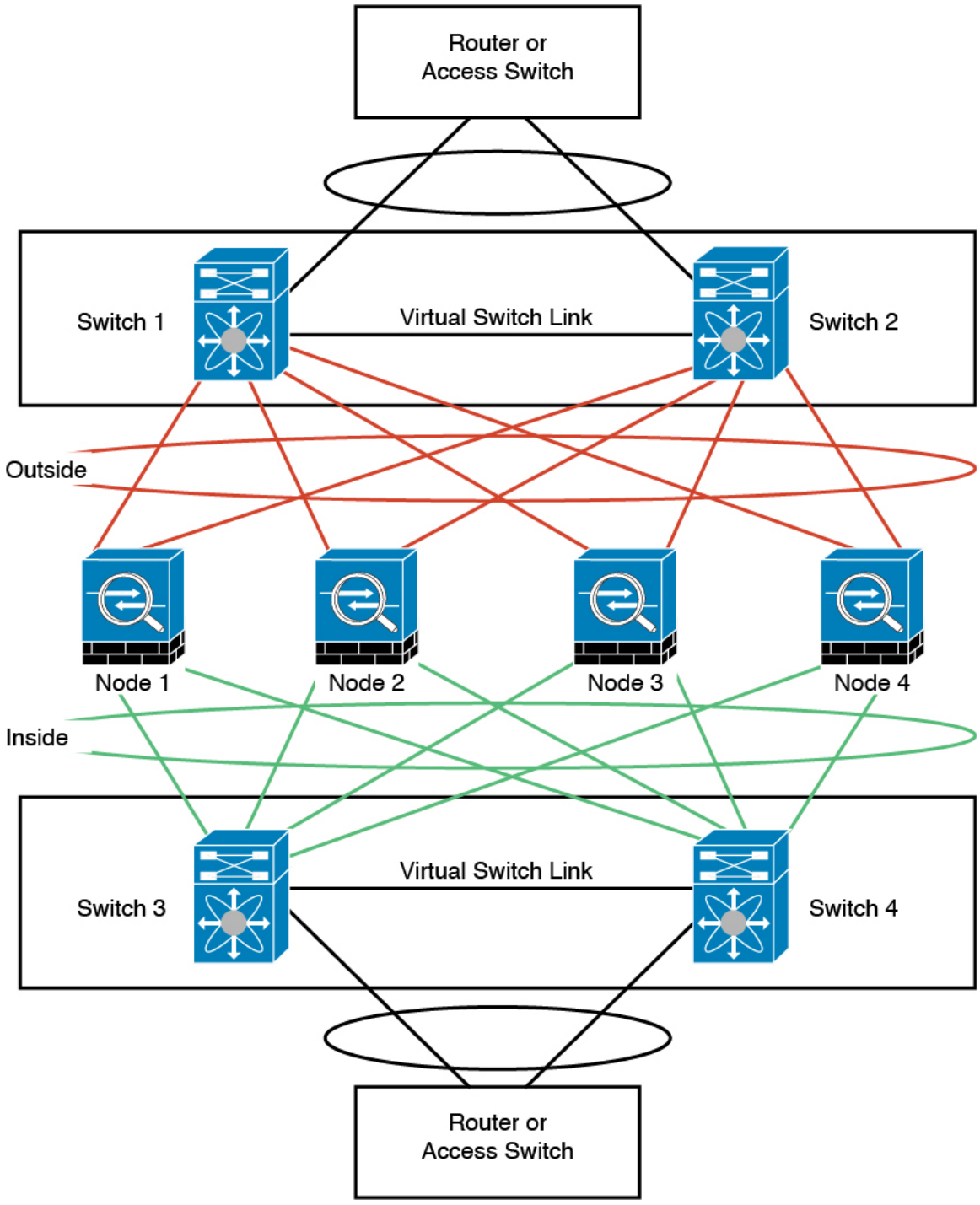


원칙은 우선 채널에 있는 액티브 포트의 수를 최대화하고, 그다음에는 액티브 제어 포트의 수와 액티브 데이터 포트의 수가 균형을 이루도록 유지하는 것입니다. 클러스터에 5번째 유닛이 참가할 경우 모든 유닛 간의 트래픽이 균일하게 조정되지 않습니다.

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 및 클러스터링

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.

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.

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 서

로 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 소유자에게 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.

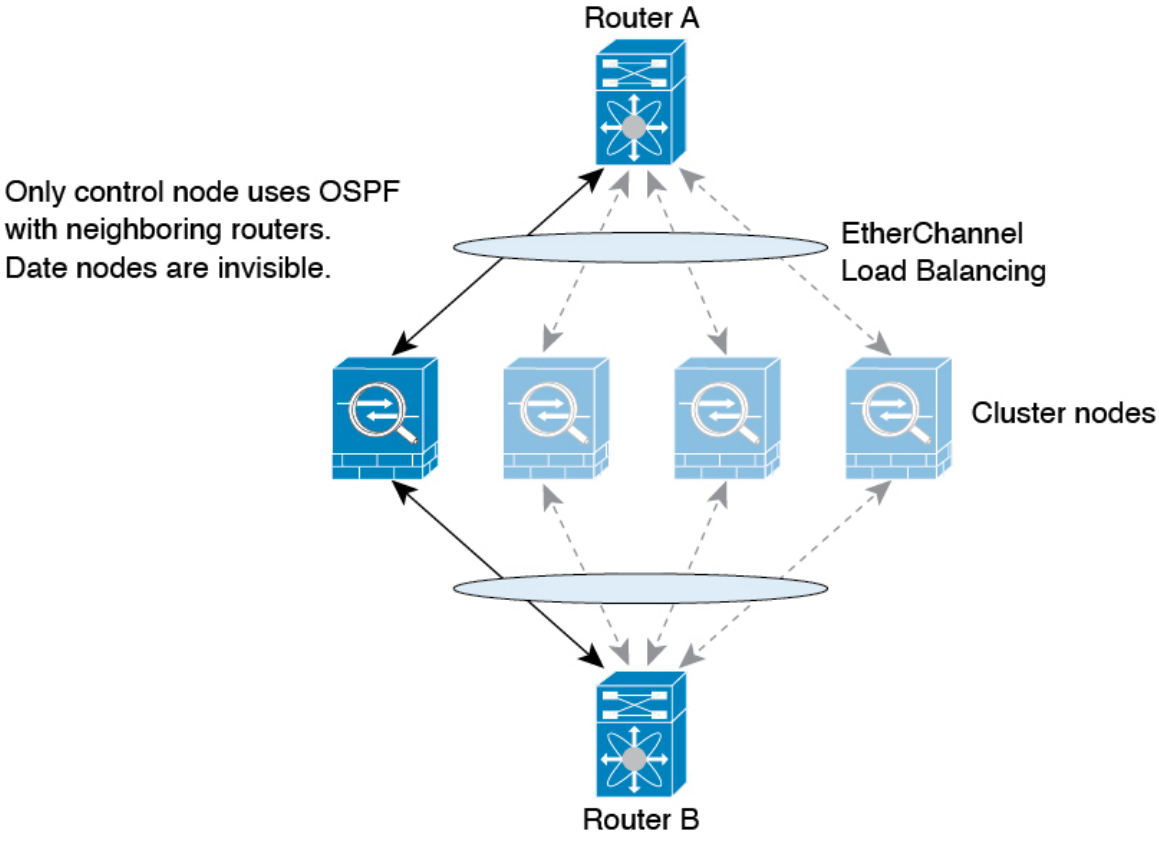
- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
  - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 노드에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서 호스트의 트래픽이 3개 노드 모두에 로드 밸런싱되는 경우 각 노드에 하나씩 3개의 블록이 할당될 수 있습니다.
  - 백업 풀의 백업 노드에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
  - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 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.

Spanned EtherChannel

라우팅 프로세스는 제어 노드에서만 실행되며, 제어 노드를 통해 경로가 파악되고 데이터 노드에 복제됩니다. 라우팅 패킷이 데이터 노드에 전송되면 해당 패킷은 제어 노드에 리디렉션됩니다.

그림 *26:* 클러스터링의 동적 라우팅



데이터 노드가 제어 노드에서 경로를 학습하면 각 노드에서는 전달과 관련된 결정을 독립적으로 수행합니다.

OSPF LSA 데이터베이스는 제어 노드에서 데이터 노드로 동기화되지 않습니다. 제어 노드 전환이 있을 경우, 인접한 라우터에서 재시작을 탐지하며 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.

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.

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 노드에서만 VPN 연결을 지원합니다.

참고 원격 액세스 VPN은 클러스터링으로 지원되지 않습니다.

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

VPN 터널을 스팬 EtherChannel 주소에 연결할 경우 연결이 제어 노드에 자동으로 전달됩니다.

VPN 관련 키 및 인증서는 모든 노드에 복제됩니다.

성능 확장 요소

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

- 통합 처리량의 70%
- 최대 연결 수의 60%
- 초당 연결 수의 50%

제어 노드 선택

클러스터의 노드는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 제어 노드를 선택합니다.

1. 노드에 클러스터링을 사용할 경우(또는 이미 사용 설정된 클러스터링을 처음 시작할 경우), 선택 요청이 3초마다 전송됩니다.
2. 다른 노드의 우선순위가 더 높을 경우 해당 노드가 선택 요청에 응답하게 됩니다. 우선순위는 1에서 100까지 설정되며 1이 가장 높은 우선순위입니다.
3. 45초 후에 우선순위가 더 높은 다른 노드에서 응답을 받지 못한 노드는 제어 노드가 됩니다.

참고 가장 우선순위가 높은 노드가 공동으로 여러 개인 경우, 클러스터 노드 이름과 일련 번호를 사용하여 제어 노드를 결정합니다.

4. 노드가 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 노드가 자동으로 제어 노드가 되는 것은 아닙니다. 기존 제어 노드는 응답이 중지되지 않는 한 항상 제어 노드로 유지되며 응답이 중지될 때에 새 제어 노드가 선택됩니다.
5. 제어 노드가 일시적으로 여러 개 있는 "스플릿 브레인" 시나리오에서는 우선 순위가 가장 높은 노드가 역할을 유지하는 반면 다른 노드는 데이터 노드 역할로 돌아갑니다.

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

클러스터 내의 고가용성

클러스터링에서는 노드 및 인터페이스의 상태를 모니터링하고 노드 간의 연결 상태를 복제하여 고가용성을 제공합니다.

노드 상태 모니터링

각 노드는 클러스터 제어 링크를 통해 브로드 캐스트 heartbeat 패킷을 주기적으로 전송합니다. 제어 노드가 시간 초과 기간 내에 데이터 유닛에서 heartbeat 패킷 또는 기타 패킷을 수신하지 않는 경우, 제어 노드는 클러스터에서 데이터 노드를 제거합니다. 데이터 노드가 제어 노드에서 패킷을 수신하지 않으면 나머지 노드에서 새 제어 노드가 선택됩니다.

네트워크 장애로 인해 노드가 실제로 장애가 발생한 것이 아니라 클러스터 제어 링크를 통해 노드가 서로 연결할 수 없는 경우, 클러스터는 격리된 데이터 노드가 자체 제어 노드를 선택하는 "스플릿 브레인" 시나리오로 전환될 수 있습니다. 예를 들어 두 클러스터 위치 간에 라우터가 실패하면 위치 1의 원래 제어 노드가 클러스터에서 위치 2 데이터 노드를 제거합니다. 한편, 위치 2의 노드는 자체 제어 노드를 선택하고 자체 클러스터를 구성합니다. 이 시나리오에서는 비대칭 트래픽이 실패할 수 있습

니다. 클러스터 제어 링크가 복원되면 우선 순위가 더 높은 제어 노드가 제어 노드의 역할을 유지합니다.

자세한 내용은 제어 노드 선택, 45 페이지를 참조하십시오.

인터페이스 모니터링

각 노드에서는 사용 중인 모든 명명된 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 제어 노드에 보고합니다.

- 스팬 EtherChannel — 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 노드에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인합니다. 상태가 제어 노드에 보고됩니다.

모든 물리적 인터페이스(주요 EtherChannel)가 기본적으로 모니터링됩니다. 명명된 인터페이스만 모니터링될 수 있습니다. 예를 들어, 명명된 EtherChannel은 장애가 발생한 것으로 간주되지 않아야 합니다. 즉, EtherChannel의 모든 멤버 포트가 클러스터 제거를 트리거하지 못해야 합니다.

노드의 모니터링된 인터페이스에 장애가 발생하면 클러스터에서 해당 노드가 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 에 따라, 그리고 해당 노드가 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. , 설정된 멤버에 대한 인터페이스가 중지되면 ASA에서는 9초 후에 해당 멤버를 제거합니다. ASA에서는 노드가 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 ASA가 클러스터에서 제거되지 않습니다.

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.

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	—
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.

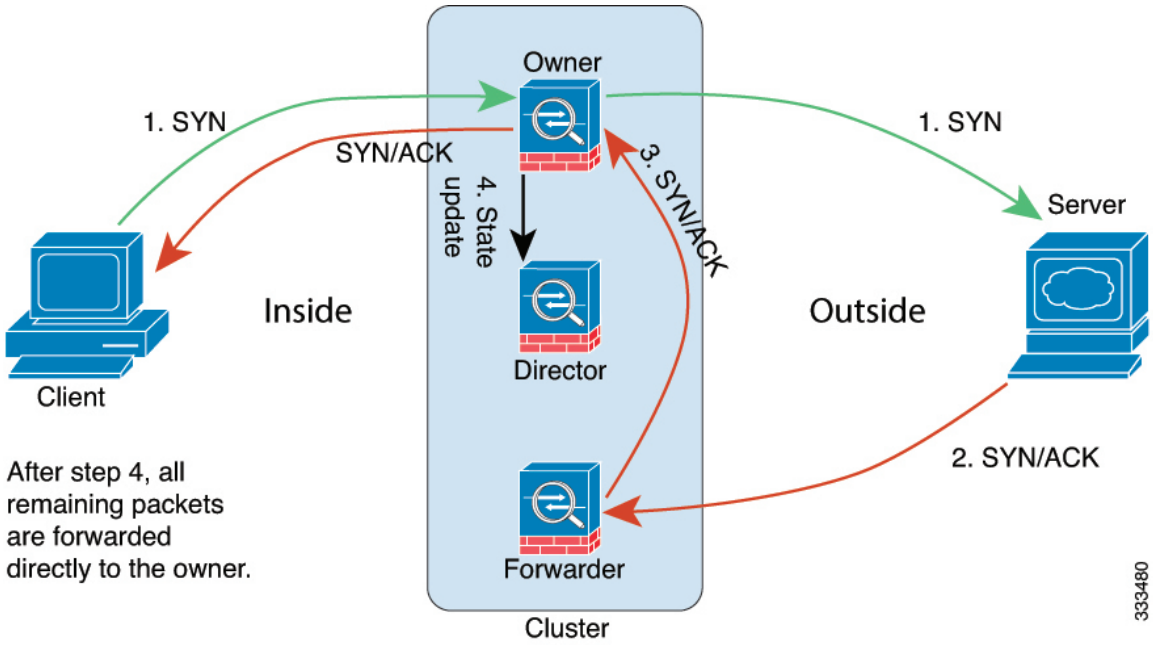
- 프래그먼트 소유자 - 프래그먼트화된 패킷의 경우 프래그먼트를 수신하는 클러스터 노드가 프래그먼트 소스 IP 주소, 대상 IP 주소 및 패킷 ID의 해시를 사용하여 프래그먼트 소유자를 결정합니다. 그런 다음 모든 프래그먼트가 클러스터 제어 링크를 통해 프래그먼트 소유자에게 전달됩니다. 첫 번째 프래그먼트만 스위치 로드 밸런싱 해시에 사용되는 5 튜플을 포함하기 때문에 프래그먼트는 다른 클러스터 노드로 로드 밸런싱될 수 있습니다. 다른 프래그먼트는 소스 및 대상 포트를 포함하지 않으며 다른 클러스터 노드에 로드 밸런싱될 수 있습니다. 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.

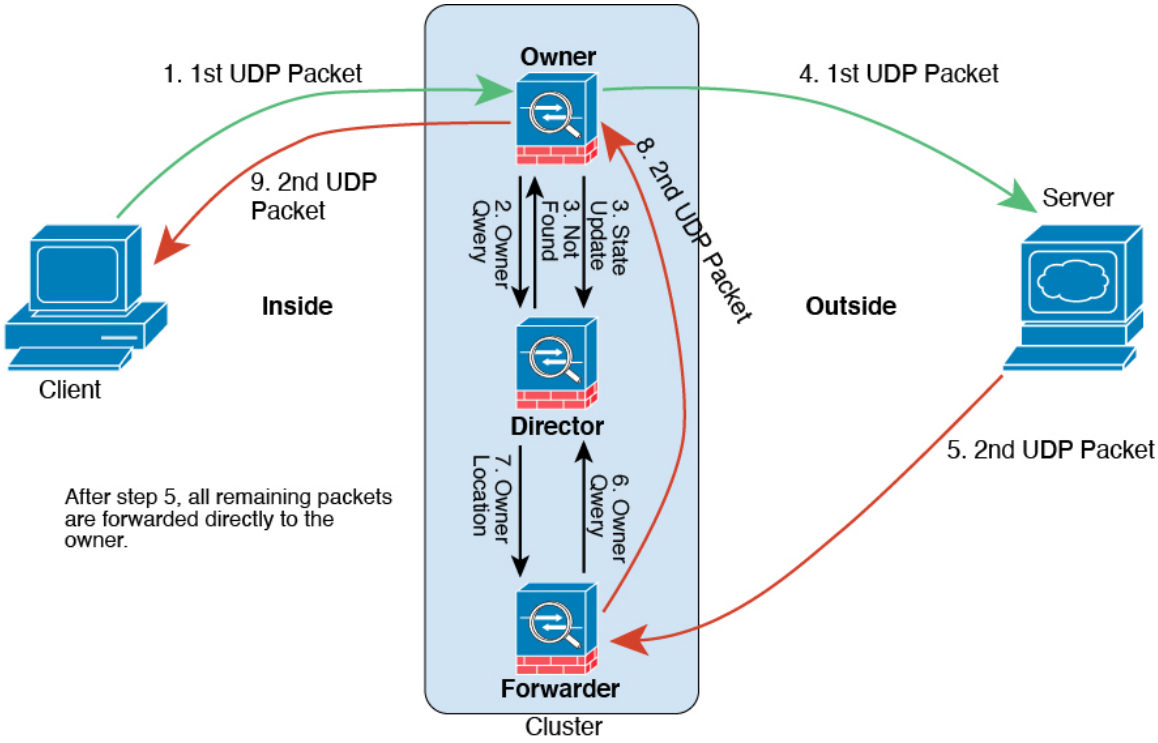


1. SYN 패킷은 클라이언트에서 시작되고 FTD에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 FTD에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 FTD는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 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 ***27: 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
Secure Firewall 3100 클러스터링	7.1	Secure Firewall 3100은 최대 8개의 노드에 대해 Spanned EtherChannel 클러스터링을 지원합니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add Cluster(**클러스터 추가**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **More(**더 보기**)** 메뉴 • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 지원되는 플랫폼: Secure Firewall 3100