고가용성

다음 주제에서는 위협 방어의 고가용성을 달성하기 위해 액티브/스탠바이 페일오버를 구성하는 방법을 설명합니다.

Secure Firewall Threat Defense 고가용성 정보

고가용성 또는 장애 조치를 구성하려면 두 개의 동일한 threat defense디바이스가 장애 조치 전용 링크 또는 경우에 따라 상태 링크와 각각 연결되어야 합니다. threat defense는 한 개의 유닛이 액티브 유닛으로 트래픽을 통과하는 Active/Standby(액티브/스탠바이) 장애 조치를 지원합니다. 스탠바이 유닛은 능동적으로 트래픽을 전달하지 않지만, 액티브 유닛에서 컨피그레이션 및 기타 상태 정보를 동기화합니다. 장애 조치가 일어나면 액티브 유닛은 스탠바이 유닛으로 장애 조치를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다.

액티브 유닛의 상태(하드웨어, 인터페이스, 소프트웨어 및 환경 상태)를 모니터링하여 특정 페일오버 조건이 충족되는지 확인합니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다.

참고 고가용성은 퍼블릭 클라우드에서 실행되는 threat defense virtual에서 지원되지 않습니다.

고가용성 시스템 요구 사항

이 섹션에서는 고가용성 구성에서 위협 방어 디바이스의 하드웨어, 소프트웨어 및 라이선스 요구 사항에 대해 설명합니다.

하드웨어 요구 사항

고가용성 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 모델이어야 합니다. 또한 컨테이너 인스턴스에 동일한 리소스 프로파일 속성을 사용해야 합니다.

  Firepower 9300의 경우 고가용성은 동일한 유형의 모듈 간에만 지원되지만, 두 섀시는 혼합된 모듈을 포함할 수 있습니다. 각 섀시에 SM-56, SM-48 및 SM-40이 있는 경우를 예로 들 수 있습니다. SM-56 모듈 간, SM-48 모듈 간, SM-40 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

  고가용성 쌍을 management center에 추가한 후 리소스 프로파일을 변경하는 경우 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **System(**시스템**)** > **Inventory(**인벤토리**)**대화 상자에서 각 유닛의 인벤토리를 업데이트합니다.

- 인터페이스 개수와 유형이 같아야 합니다.

  의 Firepower 4100/9300 섀시의 경우, 고가용성 기능을 활성화하기 전에 FXOS에서 동일하게 모든 인터페이스를 사전에 구성해야 합니다. 고가용성 기능을 활성화한 후에 인터페이스를 변경하는 경우, 스탠바이 유닛의 FXOS에서 인터페이스를 변경하고 나서 활성 유닛에서 동일하게 변경을 수행합니다.

고가용성 구성에서 플래시 메모리 크기가 다른 유닛을 사용 중인 경우, 플래시 메모리 용량이 작은 유닛에 소프트웨어 이미지 파일 및 구성 파일을 수용할 수 있는 충분한 공간이 있는지 확인해야 합니다. 그렇지 않을 경우 플래시 메모리 용량이 큰 유닛에서 플래시 메모리 용량이 작은 유닛으로 컨피그레이션을 동기화할 수 없습니다.

소프트웨어 요구 사항

고가용성 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 방화벽 모드에 있어야 합니다(라우팅 또는 투명).
- 같은 소프트웨어 버전을 사용해야 합니다.
- management center에서 동일한 도메인 또는 그룹에 속해야 합니다.
- NTP 구성이 같아야 합니다. Threat Defense를 위한 NTP 시간 동기화 구성의 내용을 참조하십시오.
- 커밋되지 않은 변경 사항 없이 management center에서 완전히 구축되어야 합니다.
- DHCP 또는 PPPoE가 인터페이스에 구성되어 있지 않아야 합니다.
- (Firepower 4100/9300) 같은 플로우 오프로드 모드가 있으며, 둘 다 활성화하거나 비활성화해야 합니다.

고가용성 쌍의 **Threat Defense** 디바이스에 대한 라이선스 요구 사항

고가용성 구성의 두 threat defense 유닛은 모두 동일한 라이선스를 가지고 있어야 합니다.

고가용성 구성에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 라이선스 자격이 필요합니다.

고가용성을 설정하기 전에는 보조/스탠바이 디바이스에 어떤 라이선스가 할당되든 상관이 없습니다. 고가용성 설정 중에 management center은 스탠바이 유닛에 할당된 불필요한 라이선스를 해제하고 기본/액티브 유닛에 할당된 것과 동일한 라이선스로 교체합니다. 예를 들어 액티브 유닛에는 Essentials 라이선스와 IPS 라이선스가 있는데 스탠바이 유닛에 Essentials 라이선스만 있는 경우, management center은 Smart Software Manager와 통신하여 스탠바이 유닛의 어카운트에서 사용 가능한 IPS 라이선스를 가져옵니다. 라이선스에 포함되어 있는 구매한 엔타이틀먼트가 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다.

페일오버 및 스테이트풀 페일오버 링크

장애 조치 링크 및 스테이트풀 장애 조치 링크(선택 사항)는 2개 유닛 간의 전용 연결입니다. Cisco에서는 페일오버 링크 또는 스테이트 풀 페일오버 링크의 두 디바이스 간에 같은 인터페이스 사용을 권장합니다. 예를 들어 페일오버 링크에서 device 1에 eth0를 사용한다면, device 2에서도 같은 인터페이스(eth0)를 사용해야 합니다.

페일오버 링크

장애 조치 쌍의 유닛 2개에서는 장애 조치 링크를 통해 지속적으로 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.

장애 조치 링크 데이터

다음 정보는 페일오버 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이)
- Hello 메시지(keep-alives)
- 네트워크 링크 상태
- MAC 주소 교환
- 컨피그레이션 복제 및 동기화

장애 조치 링크에 대한 인터페이스

사용되지 않는 데이터 인터페이스(물리적 EtherChannel)는 모두 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다.또한 다중 인스턴스 모드에 대한 섀시에 정의되어 있는 하위 인터페이스를 제외하고 하위 인터페이스를 사용할 수 없습니다. 장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능).

threat defense에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.또한 데이터와 장애 조치 링크에 대해 동일한 상위에서 별도의 하위 인터페이스를 사용할 수 없습니다(다중 인스턴스 새시 하위 인터페이스만 해당). 페일오버 링크용으로 새시 하위 인터페이스를 사용하는 경우에는 해당 상위 인터페이스의 모든 하위 인터페이스와 상위 인터페이스 자체가 페일오버 링크로 사용되도록 제한됩니다.

참고 EtherChannel 페일오버 또는 상태 링크로 사용하는 경우, 고가용성을 설정하기 전에 동일한 멤버 인터페이스를 사용하는 동일한 EtherChannel 가 두 디바이스에 있는지 확인해야 합니다.

장애 조치 링크에 대한 다음 지침을 참조하십시오.

- Firepower 4100/9300-페일오버 및 상태 링크를 함께 사용하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다.
- 기타 모델 — 1GB 인터페이스는 통합된 장애 조치 및 상태 링크에 충분한 크기입니다.

교체 빈도는 유닛 보류 시간과 같습니다.

참고 구성이 크고 유닛 보류 시간이 짧은 경우 멤버 인터페이스를 번갈아 가며 사용하면 보조 유닛이 참가/다시 참가하지 못할 수 있습니다. 이 경우 보조 유닛이 조인될 때까지 멤버 인터페이스 중 하나를 비활성화합니다.

장애 조치 링크로 사용된 EtherChannel의 경우, EtherChannel의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

장애 조치 링크 연결

다음 2가지 방법 중 하나를 사용하여 장애 조치 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 위협 방어 디바이스의 장애 조치 인터페이스로 사용합니다.
- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다.

유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

스테이트풀 페일오버 링크

스테이트풀 장애 조치를 사용하려면 연결 상태 정보를 전달할 스테이트풀 장애 조치 링크(상태 링크라고도 함)를 구성해야 합니다.

장애 조치 링크 공유

장애 조치 링크를 공유하는 방법은 인터페이스를 보호하는 가장 좋은 방법입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다.

스테이트풀 장애 조치 링크에 대한 전용 인터페이스

상태 링크에 전용 데이터 인터페이스(물리적 또는 EtherChannel)를 사용할 수 있습니다. 전용 상태 링크의 요구 사항은 장애 조치 링크에 대한 인터페이스, 3 페이지의 내용, 그리고 상태 링크 연결에 대한 정보는 장애 조치 링크 연결, 4 페이지의 내용을 참조하십시오.

장거리 페일오버를 사용할 경우 최적의 성능을 보장하려면 페일오버 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 페일오버 메시지의 재전송으로 인해 성능이 다소 저하됩니다.

페일오버 및 데이터 링크 중단 방지

페일오버 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 페일오버 링크가 중단될 경우 threat defense 디바이스는 데이터 인터페이스를 사용하여 페일오버가 필요한지 여부를 확인할 수 있습니다. 그런 다음 페일오버 링크 상태가 복원될 때까지는 페일오버 작업이 보류됩니다.

복원력이 뛰어난 페일오버 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 **1** — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 threat defense 디바이스 간의 페일오버 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 threat defense 디바이스 모두 액티브 상태가 됩니다. 따라서 아래의 그림에 있는 다음 2가지 연결 방법은 권장하지 않습니다.

그림 ***1:*** 단일 스위치로 연결 - 권장하지 않음

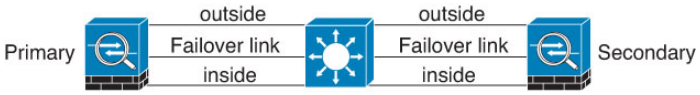
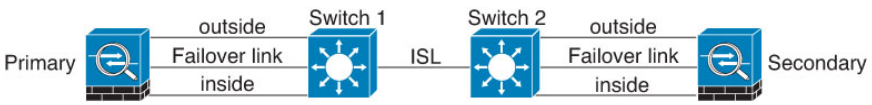


그림 ***2:*** 이중 스위치로 연결 - 권장하지 않음



시나리오 **2** - 권장함

페일오버 링크에서는 데이터 인터페이스와 같은 스위치를 사용하지 않는 것이 좋습니다. 대신 다음 그림에 나와 있는 것처럼 다른 스위치를 사용하거나 다이렉트 케이블을 사용하여 페일오버 링크에 연결합니다.

그림 *3:* 다른 스위치로 연결

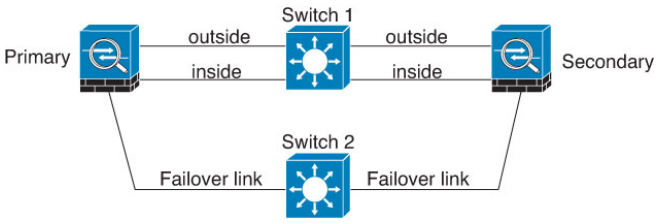
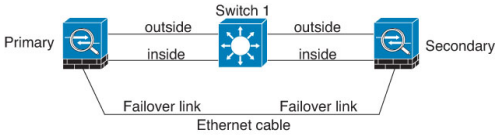


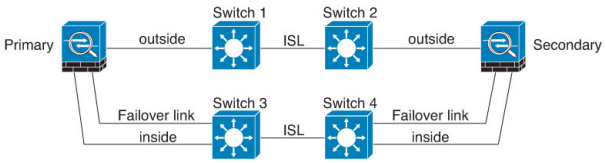
그림 *4:* 케이블로 연결



시나리오 **3** — 권장

threat defense 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 페일오버 링크는 이러한 스위치 중 하나에 연결될 수 있으며 다음 그림에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 *5:* 보안 스위치로 연결



시나리오 **4** — 권장

가장 안정적인 페일오버 컨피그레이션에서는 다음 그림에 나와 있는 것처럼 페일오버 링크에서 이중 인터페이스를 사용합니다.

그림 *6:* 이중 인터페이스로 연결

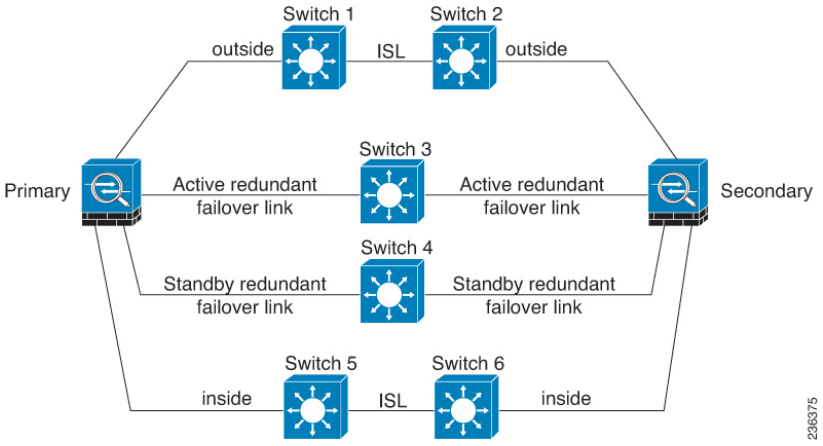
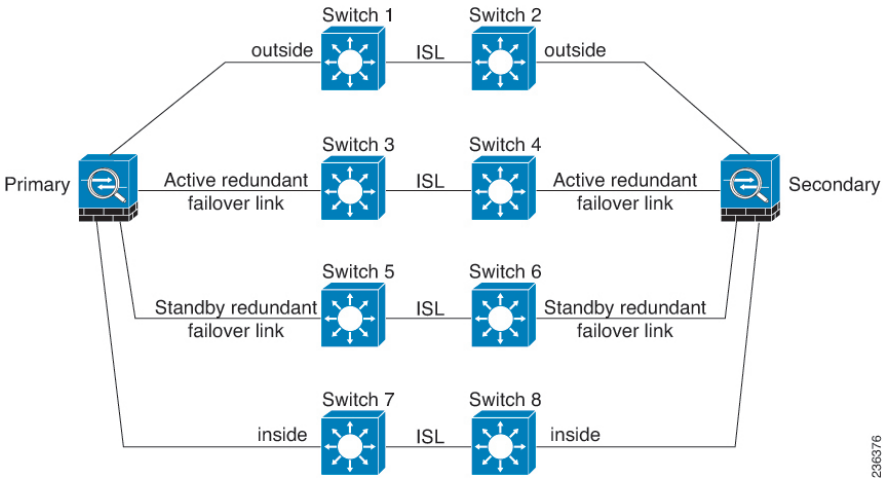


그림 7: 스위치 간 링크로 연결



MAC 주소와 IP 주소 - 고가용성

인터페이스를 구성할 때는 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정할 수 있습니다. 일반적으로 페일오버가 발생할 때는 활성 IP 주소와 MAC 주소가 새 액티브 유닛에 승계됩니다. 네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

참고 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다. 관리 목적으로 해당 인터페이스에서 스탠바이 유닛에 연결할 수도 없습니다.

상태 링크의 IP 주소와 MAC 주소는 장애 조치 시 변경되지 않습니다.

액티브/스탠바이 IP 주소와 MAC 주소

액티브/스탠바이 고가용성의 경우 페일오버 이벤트가 발생하는 동안의 IP 주소 및 MAC 주소 사용법은 다음 설명을 참조하십시오.

1. 액티브 유닛은 항상 기본 유닛의 IP 주소와 MAC 주소를 사용합니다.
2. 액티브 유닛에서 장애 조치가 수행될 때 스탠바이 유닛에서는 장애 발생 유닛의 IP 주소와 MAC 주소를 사용해 트래픽 전달을 시작합니다.
3. 장애 발생 유닛은 다시 온라인으로 설정되면 스탠바이 상태가 되며 스탠바이 IP 주소와 MAC 주소를 승계합니다.

하지만 기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 기본 유닛이 사용 가능해지면 보조(액티브) 유닛이 MAC 주소를 기본 유닛의 주소로 변경하므로 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다.

시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 위협 방지 디바이스에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

가상 **MAC** 주소

위협 방지 디바이스에서는 여러 가지 방법으로 가상 MAC 주소를 구성할 수 있습니다. 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

다중 인스턴스 기능의 경우 FXOS 섀시에서는 모든 인터페이스에 대해 기본 MAC 주소만 자동 생성합니다. 생성된 MAC 주소를 기본 및 보조 MAC 주소가 모두 포함된 가상 MAC 주소로 덮어쓸 수 있습니다. 보조 MAC 주소를 반드시 사전 정의해야 하는 것은 아니지만, 보조 MAC 주소를 설정하면 새 보조 유닛 하드웨어 사용 시 to-the-box 관리 트래픽이 중단되지 않도록 보장할 수 있습니다.

스테이트풀 페일오버

스테이트풀 장애 조치 동안 활성화한 경우, 액티브 유닛에서는 연결당 상태 정보를 스탠바이 유닛. 장애 조치가 일어난 후에는 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션이 없어도 다시 연결하여 동일한 통신 세션을 그대로 유지할 수 있습니다.

지원 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 위협 방지 디바이스로 전달됩니다.

- NAT 변환 테이블.
- TCP 및 UDP 연결과 상태(HTTP 연결 상태 포함). 다른 유형의 IP 프로토콜과 ICMP는 새 패킷이 도착하면 새 액티브 유닛에서 설정되므로 액티브 유닛에서 구문 분석되지 않습니다.
- Snort 연결 상태, 검사 결과 및 핀홀 정보(엄격한 TCP 적용 포함).
- ARP 테이블
- 레이어 2 브리지 테이블(브리지 그룹용)
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 시그널링 세션 및 핀홀.
- 정적 및 동적 라우팅 테이블 - 스테이트풀 페일오버는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 확인한 경로는 스탠바이 유닛의 RIB(Routing Information Base) 테이블에 유지됩니다. 페일오버 이벤트 발생 시 액티브 보조 유닛에서는 초기 규칙에 따라 기본 유닛을 미러링하므로 트래픽 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 페일오버가 끝난 직후에는 새 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP

경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.

참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스탠바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적이고 정상적인 동작입니다.

- DHCP 서버 - DHCP 주소 임대는 복제되지 않습니다. 그러나 인터페이스에 구성된 DHCP 서버는 ping을 전송하여 특정 주소가 사용 중이지 않음을 확인한 후에 DHCP 클라이언트에 해당 주소를 부여하므로 서비스에는 영향이 없습니다. 상태 정보는 DHCP 릴레이 또는 DDNS와 관련이 없습니다.
- 액세스 제어 정책 결정 - 트래픽 일치(URL, URL 카테고리, 지리위치 등), 침입 탐지, 악성코드 및 파일 유형과 관련된 결정은 페일오버 중에 그대로 유지됩니다. 그러나 페일오버 시점에서 평가 중인 연결의 경우 다음 경고가 적용됩니다.
  - AVC - 앱-ID 판정은 복제되지만 탐지 상태는 복제되지 않습니다. 페일오버가 수행되기 전에 앱-ID 판정이 완료 및 동기화되면 적절한 동기화가 수행됩니다.
  - 침입 탐지 상태 - 페일오버 시 중간 플로우 픽업이 발생하면 새 검사는 완료되지만 이전 상태는 손실됩니다.
  - 파일 악성코드 차단 - 페일오버 전에 파일 상태를 확인할 수 있어야 합니다.
  - 파일 유형 탐지 및 차단 - 페일오버 전에 파일 유형이 식별되어야 합니다. 원래 액티브 디바이스가 파일을 식별하는 중에 페일오버가 수행되면 파일 유형이 동기화되지 않습니다. 따라서 파일 정책에서 해당 파일 유형을 차단하더라도 새 액티브 디바이스는 파일을 다운로드합니다.
- ID 정책의 사용자 ID 결정(ISE 세션 디렉터리에서 수동으로 수집한 사용자-IP 주소 매핑과 종속 포털을 통한 액티브 인증 포함). 페일오버 시점에서 활성 인증 중인 사용자의 경우 다시 인증하라는 프롬프트가 표시될 수 있습니다.
- 네트워크 AMP - 클라우드 조회는 각 디바이스와 독립적으로 작동하므로 페일오버는 일반적으로 이 기능에 영향을 주지 않습니다. 구체적으로 말씀드리면,
  - 서명 조회 - 파일 전송 중에 페일오버가 수행되면 파일 이벤트가 생성되지 않으며 탐지도 수행되지 않습니다.
  - 파일 스토리지 - 파일을 저장하고 있을 때 페일오버가 수행되면 해당 파일은 원래 액티브 디바이스에 저장됩니다. 파일을 저장하는 중에 원래 액티브 디바이스가 중단된 경우에는 파일이 저장되지 않습니다.
  - 파일 사전 분류(로컬 분석) - 사전 분류 중에 페일오버가 수행되면 탐지에 실패합니다.

- 파일 동적 분석(클라우드 연결) - 페일오버가 수행되는 경우 시스템이 클라우드에 파일을 제출할 수 있습니다.
- 아카이브 파일 지원 - 분석 중에 페일오버가 수행되면 시스템에서 파일/아카이브에 대한 가시성을 잃게 됩니다.
- 맞춤형 차단 — 페일오버가 수행되면 이벤트가 생성되지 않습니다.

- 보안 인텔리전스 결정. 그러나 페일오버 시점에서 처리 중인 DNS 기반 결정은 완료되지 않습니다.
- RA VPN - 원격 액세스 VPN 최종 사용자는 페일오버 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 페일오버 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.
- 모든 연결 중에서 설정된 연결만 스탠바이 ASA에 복제됩니다.

지원되지 않는 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 위협 방지 디바이스로 전달되지 않습니다.

- GREv0 및 IPv4-in-IP가 아닌 일반 텍스트 터널의 세션. 터널 내의 세션은 복제되지 않으며, 새 액티브 노드는 기존 검사 판정을 재사용하여 정확한 정책 규칙 일치 여부를 확인할 수 없습니다.
- 암호 해독된 TLS/SSL 연결 - 암호 해독 상태가 동기화되지 않고 만약 액티브 유닛에 장애가 발생하면 암호 해독된 연결이 재설정됩니다. 새 활성 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(TLS/SSL 암호 해독 안 함 규칙 작업과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.
- TCP 상태 우회 연결
- 멀티캐스트 라우팅.

고가용성에 대한 브리지 그룹 요구 사항

브리지 그룹 사용 시 고가용성에 대해 특별히 고려해야 할 사항이 있습니다.

액티브 유닛이 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 스위치 포트가 토폴로지 변경을 인지하는 경우 30초~50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 브리지 그룹 멤버 인터페이스에서 트래픽 손실을 방지하려면 다음 해결 방법 중 하나를 구성할 수 있습니다.

- 스위치 포트는 액세스 모드입니다 - 스위치에서 STP PortFast 기능을 활성화합니다.

```
interface interface_id
  spanning-tree portfast
```

PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 스위치 포트가 트렁크 모드 상태이거나 STP PortFast를 활성화할 수 없는 경우 페일오버 기능 또는 STP 안정성에 영향을 줄 수 있는 다음 해결 방법을 선택할 수 있습니다.
  - 브리지 그룹 및 멤버 인터페이스에 인터페이스 모니터링을 비활성화합니다.
  - 페일오버 기준에서 인터페이스 대기 시간을 큰 값으로 늘려 유닛 페일오버 전 STP를 통합시킵니다.
  - 스위치가 STP를 인터페이스 대기 시간보다 빠르게 통합하도록 STP 타이머를 감소시킵니다.

장애 조치 상태 모니터링

위협 방어 디바이스에서는 각 유닛의 전체 상태 및 인터페이스 상태를 모니터링합니다. 이 섹션에는 위협 방어 디바이스에서 각 유닛의 상태를 확인하기 위해 테스트를 수행하는 방법에 대한 정보가 포함되어 있습니다.

유닛 상태 모니터링

threat defense 디바이스에서는 hello 메시지가 있는 장애 조치 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 장애 조치 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 장애 조치 링크를 비롯한 각 데이터 인터페이스에 LANTEST 메시지를 전송하여 피어의 응답 여부를 확인합니다. threat defense 디바이스에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다. 아래의 가능한 조치를 참조하십시오.

- threat defense 디바이스에서 장애 조치 링크에 대한 응답을 수신하지 못할 경우 장애 조치가 이루어지지 않습니다.
- threat defense 디바이스에서 장애 조치 링크에 대한 응답은 수신하지 못했으나 데이터 인터페이스에 대한 응답은 수신한 경우, 유닛에서 장애 조치를 수행하지 않습니다. 페일오버 링크가 실패한 것으로 표시됩니다. 페일오버 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버할 수 없으므로 최대한 빨리 페일오버 링크를 복원해야 합니다.
- threat defense 디바이스에서 인터페이스에 대한 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 실패한 것으로 분류합니다.

인터페이스 모니터링

15초 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 인터페이스 테스트가 실행됩니다. 인터페이스에 대한 단일 인터페이스 테스트가 실패하였으나 다른 유닛에 있는 이 동일한 인터페이스에서는 지속적으로 트래픽을 전달할 수 있다면, 해당 인터페이스는 오류가 발생한 것으로 간주되며 디바이스는 테스트를 중단합니다.

오류가 발생한 인터페이스 수에 정의한 임계값이 충족된다면(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **High Availability(**고가용성**)** > **Failover Trigger Criteria(**페일오버 트리거 기준**))**를 참조하십시오. 액티브 유닛이 대기 유닛보다 오류가 발생한 인터페이스가 많으면 페일오버가 발생합니다. 두 유닛의 인터페이스가 모두 실패하면, 두 인터페이스 모두 'Unknown(알 수 없음)' 상태가 되며 페일오버 인터페이스 정책에서 정의하는 페일오버 한도에 합산되지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 장애 임계값이 더 이상 충족되지 않을 경우 장애가 발생한 디바이스는 스탠바이 모드로 돌아갑니다.

인터페이스에 구성된 IPv4 및 IPv6 주소가 없는 경우 디바이스에서는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다. 인터페이스에 IPv6 주소만 구성되어 있으면 디바이스에서는 ARP 대신 IPv6 네이버 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 ping 테스트의 경우 디바이스에서는 IPv6 모든 노드 주소를 사용합니다(FE02::1).

인터페이스 테스트

위협 방어 디바이스에서는 다음과 같은 인터페이스 테스트를 사용합니다. 각 테스트 시간은 기본적으로 1.5초.

1. 링크 작동/중단 테스트 - 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 중단되었는지 여부를 나타내며, 디바이스에서는 이 상태를 실패로 간주하고 테스트를 중단합니다. 작동 상태일 경우 디바이스에서는 네트워크 활동 테스트를 수행합니다.
2. 네트워크 활동 테스트 - 수신된 네트워크 활동 테스트입니다. 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 유닛에서 테스트 도중 적합한 패킷을 수신하는 즉시, 인터페이스는 작동 중으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛에서도 트래픽을 수신하지 못하면, 디바이스에서는 ARP 테스트를 시작합니다.
3. ARP 테스트 - 성공적인 ARP 응답에 대한 테스트입니다. 각 유닛은 ARP 테이블의 가장 최근 항목에 있는 IP 주소에 대한 단일 ARP 요청을 전송합니다. 유닛이 테스트 중에 ARP 응답이나 기타 네트워크 트래픽을 수신한다면, 인터페이스는 작동하는 것으로 간주됩니다. 유닛이 ARP 회신을 수신하지 못한다면, 디바이스는 ARP 테이블의 다음 항목에 있는 IP 주소에 대한 단일 ARP 요청을 전송합니다. 유닛이 테스트 중에 ARP 응답이나 기타 네트워크 트래픽을 수신한다면, 인터페이스는 작동하는 것으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛에서도 트래픽을 수신하지 못하면, 디바이스에서는 Broadcast Ping(브로드캐스트 핑) 테스트를 시작합니다.
4. Broadcast Ping(브로드캐스트 핑) 테스트 - 성공적인 핑 회신에 대한 테스트입니다. 각 유닛은 브로드캐스트 핑을 보낸 다음 수신된 모든 패킷을 계산합니다. 유닛이 테스트 도중 패킷을 수신하면, 인터페이스는 작동 중으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛도 트래픽을 수신하지 않으면, 테스트는 ARP 테스트와 함께 다시 시작됩니다. 두 유닛 모두 ARP 및 Broadcast Ping(브로드캐스트 핑) 테스트에서 트래픽을 계속 수신하지 못하면, 테스트는 영구적으로 계속 실행됩니다.

인터페이스 상태

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.

- Normal (Waiting)(일반(대기 중)) — 인터페이스가 작동하지만 피어 유닛의 해당 인터페이스에서 hello 패킷을 아직 받지 않았습니다.
- Normal (Not-Monitored)(일반(모니터링되지 않음)) —인터페이스가 작동하지만 장애 조치 프로세스에서 모니터링되지 않습니다.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- Link Down (Waiting)(연결 해제(대기 중)) — 인터페이스 또는 VLAN이 관리상 작동 중단되었으며 피어 유닛의 해당 인터페이스에서 hello 패킷을 아직 받지 않았습니다.
- Link Down (Not-Monitored)(연결 해제(모니터링되지 않음)) — 인터페이스 또는 VLAN이 관리상 작동 중단되었지만 장애 조치 프로세스에서 모니터링되지 않습니다.
- No Link(연결 없음) - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- No Link (Waiting)(연결 없음(대기 중)) — 인터페이스의 물리적 링크가 작동 중단되었으며 피어 유닛의 해당 인터페이스에서 hello 패킷을 아직 받지 않았습니다.
- No Link (Not-Monitored)(연결 없음(모니터링되지 않음)) — 인터페이스의 물리적 링크가 작동 중단되었지만 장애 조치 프로세스에서 모니터링되지 않습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

장애 조치 트리거 및 탐지 시간

다음 이벤트는 Firepower 고가용성 쌍에서 페일오버를 트리거합니다.

- 활성 유닛의 Snort 인스턴스 중 50 % 이상이 다운되었습니다.
- 활성 유닛의 디스크 공간이 90 % 이상 찼습니다.
- **no failover active(**활성 페일오버 없음**)** 명령이 활성 유닛에서 실행되거나 **failover active(**활성 페일오버**)** 명령이 대기 유닛에서 실행됩니다.
- 대기 유닛보다 활성 유닛에 더 많은 실패 인스턴스가 있습니다.
- 활성 디바이스의 인터페이스 오류가 구성된 임계 값을 초과합니다.

  기본적으로 하나의 인터페이스에 오류가 발생하면 페일오버가 실행됩니다. 인터페이스 수에 대한 임계값 또는 페일오버가 발생하기 위해 실패해야 하는 모니터링되는 인터페이스의 백분율을 구성하여 기본값을 변경할 수 있습니다. 활성 디바이스에서 임계값이 위반되면 페일오버가 발생합니다. 대기 디바이스에서 임계값 위반이 발생하면 유닛은 **Fail(**실패**)** 상태로 전환됩니다.

  기본 페일오버 기준을 변경하려면 전역 구성 모드에서 다음 명령을 입력합니다.

표 *1:*

명령	목적
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	기본 페일오버 기준을 변경합니다. 인터페이스의 특정 개수를 지정할 경우, *num* 인수의 지원되는 범위는 1에서 250까지입니다. 인터페이스의 백분율을 지정할 경우 *num* 인수의 지원되는 범위는 1에서 100까지입니다.

다음 표에는 페일오버를 트리거하는 이벤트 및 관련 장애 탐지 타이밍이 나와 있습니다. 장애 조치가 발생하는 경우 고가용성 쌍과 관련된 다양한 작업과 함께 Message Center에서 장애 조치 이유를 확인할 수 있습니다. 이러한 임계값을 지정된 최소-최대 범위 내의 값으로 구성할 수 있습니다.

표 *2: Threat Defense* 장애 조치 시간

장애 조치 트리거 이벤트	최소	기본	최대
활성 유닛의 전원이 끊기거나, 하드웨어가 다운되거나, 소프트웨어가 다시 로드되거나 충돌합니다. 이러한 상황이 발생하면 모니터링되는 인터페이스 또는 페일오버 링크에서 hello 메시지를 수신하지 않습니다.	800밀리초	15초	45초
액티브 유닛 인터페이스 물리적의 연결이 해제됩니다.	500밀리초	5초	15초
액티브 유닛 인터페이스가 작동하지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

액티브/스탠바이 페일오버 정보

액티브/스탠바이 페일오버에서는 스탠바이 위협 방지 디바이스를 사용해 장애가 발생한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하는 경우 스탠바이 유닛이 액티브 유닛이 됩니다.

기본/보조 역할 및 액티브/스탠바이 상태

액티브/스탠 바이 페일오버를 설정할 때는 한 유닛을 기본 유닛으로, 다른 유닛을 보조 유닛으로 구성합니다. 컨피그레이션 중에는 기본 유닛의 정책이 보조 유닛에 동기화됩니다. 이 시점에서 두 유닛은 디바이스 및 정책 컨피그레이션을 위해 단일 디바이스로 작동합니다. 하지만 이벤트, 대시보드, 보고서 및 상태 모니터링의 경우에는 계속해서 별도의 디바이스로 표시됩니다.

페일오버 쌍의 두 유닛의 주된 차이점은 어느 유닛이 액티브 유닛이고 어느 유닛이 스탠바이 유닛인지와 관련 있습니다. 즉, 어떤 IP 주소를 사용하고 어떤 유닛이 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.
- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 페일오버 링크를 통해 기본 유닛의 MAC 주소를 획득할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

페일오버 이벤트

액티브/스탠바이 페일오버 시 페일오버는 유닛을 기준으로 실행됩니다.

다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 페일오버 이벤트에 적용되는 페일오버 정책(페일오버 실행 또는 페일오버 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 페일오버 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 ***3:*** 페일오버 이벤트

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 페일오버 링크에 대한 hello 메시지가 수신되지 않음
이전 액티브 유닛 복구	페일오버 없음	스탠바이 상태가 됨	작업 없음	없음

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
스탠바이 유닛 오류(전력 또는 하드웨어)	페일오버 없음	스탠바이가 실패한 것으로 표시됨	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	페일오버 링크가 실패한 것으로 표시됨	페일오버가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버를 시작하지 못하므로 최대한 빨리 페일오버 링크를 복구해야 합니다.
시작 시 페일오버 링크에 오류 발생	페일오버 없음	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	시작 시 페일오버 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	페일오버가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	페일오버	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	페일오버 없음	작업 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

구성 동기화 최적화

페일오버 일시 중단 또는 재개 후 노드가 리부팅되거나 노드가 다시 참가하는 경우 참가하는 유닛은 실행 중인 구성을 지웁니다. 액티브 유닛은 전체 구성 동기화를 위해 전체 구성을 참가하는 유닛으로 전송합니다. 액티브 유닛에 대규모 구성이 있는 경우, 참가하는 유닛에서 구성을 동기화하는 데 몇 분 정도 걸립니다.

구성 동기화 최적화 기능을 사용하면 구성 해시 값을 교환하여 조인 유닛과 액티브 유닛의 구성을 비교할 수 있습니다. 액티브 유닛과 조인 유닛 모두에서 계산된 해시가 일치하는 경우, 조인 유닛은 전체 구성 동기화를 건너뛰고 HA에 다시 조인합니다. 이 기능을 사용하면 HA 피어링 속도가 빨라지고 유지 관리 기간과 업그레이드 시간이 단축됩니다.

구성 동기화 최적화의 지침 및 제한 사항

- 구성 동기화 최적화 기능은 threat defense버전 7.2 이상에서 기본적으로 활성화됩니다.

- threat defense 다중 상황 모드는 전체 구성 동기화 중에 상황 순서를 공유하여 후속 노드 다시 조인 중에 상황 순서를 비교할 수 있도록 구성 동기화 최적화 기능을 지원합니다.
- 암호 및 페일오버 IPsec 키를 구성하는 경우 액티브 유닛과 스탠바이 유닛에서 계산되는 해시 값이 다르기 때문에 구성 동기화 최적화가 적용되지 않습니다.
- 동적 ACL 또는 SNMPv3를 사용하여 디바이스를 구성하는 경우 구성 동기화 최적화 기능이 적용되지 않습니다.
- 액티브 유닛은 기본 동작으로 플래핑 LAN 링크를 사용하여 전체 구성을 동기화합니다. 액티브 유닛과 스탠바이 유닛 간의 페일오버 플랩 중에는 구성 동기화 최적화 기능이 트리거되지 않고 전체 구성 동기화를 수행합니다.

구성 동기화 최적화 모니터링

구성 동기화 최적화 기능이 활성화된 경우 시스템 로그 메시지가 생성되어 액티브 유닛과 조인 유닛에서 계산된 해시 값이 일치하는지 여부 또는 작업 시간 초과가 만료되는지 여부를 표시합니다. 시스템 로그는 메시지는 또한 해시 요청을 전송한 시간부터 해시 응답을 가져오고 비교하는 시간까지 경과된 시간을 표시합니다.

고가용성 요구 사항 및 사전 요건

모델 지원

Secure Firewall Threat Defense

지원되는 도메인

모든

사용자 역할

관리자

네트워크 관리자

고가용성 지침

모델 지원

- Firepower 1010:
  - 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프

로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.

- 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.

참고 버전 6.5 이상이 management center 버전 6.5 이상에서 새로 설치하고 관리하는 Firepower 1010 디바이스에서 기본 인터페이스는 스위치 포트 유형이 됩니다. 스위치 포트 기능은 페일오버에 지원되지 않으므로 해당 인터페이스에서 스위치 포트를 끄고 구축을 수행한 다음 페일오버를 생성합니다. 6.5 이전 버전에서 업그레이드된 Firepower 1010 시스템의 경우, 기본 인터페이스는 이전 버전과 동일합니다.

- Firepower 9300 - 섀시 내 고가용성은 지원되지 않습니다.
- Microsoft Azure 및 Amazon Web Services와 같은 퍼블릭 클라우드 네트워크에 있는 threat defense virtual 에서는 Layer 2 연결이 필요하기 때문에 고가용성를 통해 지원되지 않습니다.

추가 지침

- 액티브 유닛에서 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하기 위해 스위치에서 STP PortFast 기능을 활성화할 수 있습니다.

  interface *interface_id* **spanning-tree portfast**

  이 해결 방법은 라우팅 모드 및 브리지 그룹 인터페이스에 모두 연결된 스위치에 적용됩니다. PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 위협 방지 디바이스 페일오버 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 페일오버 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확보한 보안 MAC 주소가 다른 보안 포트로 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.
- 액티브/스탠바이 고가용성 및 VPN IPsec 터널의 경우, VPN 터널을 통해 SNMP를 사용하여 액티브 유닛과 스탠바이 유닛을 모두 모니터링할 수는 없습니다. 스탠바이 유닛에는 활성 VPN 터널이 없으며 NMS로 전송되는 트래픽은 삭제됩니다. 암호화 기능이 있는 SNMPv3을 대신 사용하면 IPsec 터널을 사용하지 않아도 됩니다.
- 고가용성 쌍을 생성하는 동안 피어 디바이스에서 clish를 실행하면 두 피어 디바이스가 모두 알 수 없음 상태가 되며, 고가용성 구성에 실패합니다.
- 페일오버 직후 시스템 로그 메시지의 소스 주소는 몇 초 동안 페일오버 인터페이스 주소가 됩니다.

- 더 나은 통합을 위해(페일오버 중) 구성 또는 인스턴스와 연결되지 않은 HA 쌍의 인터페이스를 종료해야 합니다.
- 평가 모드에서 HA 페일오버 암호화를 구성하는 경우 시스템은 암호화에 DES를 사용합니다. 그런 다음 내보내기 호환 계정을 사용하여 디바이스를 등록하면 디바이스는 재부팅 후 AES를 사용합니다. 따라서 업그레이드를 설치한 후를 포함하여 어떤 이유로든 시스템을 재부팅하면 피어가 통신할 수 없으며 두 유닛이 모두 활성 유닛이 됩니다. 디바이스를 등록할 때까지는 암호화를 구성하지 않는 것이 좋습니다. 평가 모드에서 구성하는 경우 디바이스를 등록하기 전에 암호화를 제거하는 것이 좋습니다.
- 페일오버와 함께 SNMPv3를 사용할 때 페일오버 유닛을 교체하면 SNMPv3 사용자가 새 유닛에 복제되지 않습니다.사용자를 제거하고 다시 추가한 다음 사용자가 새 유닛에 복제하도록 강제로 구성을 재구축해야 합니다.
- threat defense는 피어와 SNMP 클라이언트 엔진 데이터를 공유하지 않습니다.
- 액세스 제어 및 NAT 규칙이 매우 많은 경우, 구성의 크기가 효율적인 구성 복제를 방해하여 스탠바이 유닛이 스탠바이 준비 상태에 도달하는 데 시간이 너무 오래 걸릴 수 있습니다. 이는 콘솔 또는 SSH 세션을 통해 복제하는 동안 스탠바이 유닛에 연결하는 기능에도 영향을 줄 수 있습니다. 구성 복제 성능을 높이려면 **asp rule-engine transactional-commit access-group** 및 **asp rule-engine transactional-commit nat** 명령을 사용하여 액세스 규칙과 NAT 모두에 대해 트랜잭션 커밋을 활성화합니다.
- 스탠바이 역할로 전환되는 고가용성 쌍의 유닛은 클럭을 액티브 유닛과 동기화합니다.

  예:

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby              Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config               Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- 고가용성(페일오버)의 유닛은 클럭을 동적으로 동기화하지 않습니다. 다음은 동기화가 발생하는 이벤트의 몇 가지 예입니다.
  - 새 HA 쌍이 생성됩니다.
  - HA가 중단되고 다시 생성됩니다.
  - 페일오버 링크를 통한 통신이 중단 및 재설정되었습니다.
  - **no failover/failover** 또는 **configure high-availability suspend/resume** (threat defense CLISH) 명령을 사용하여 페일오버 상태를 수동으로 변경했습니다.
- 플랫폼에서 실행되는 ASA/threat defense 쌍에서 동기화는 섀시가 아닌 ASA/threat defense와 같은 애플리케이션에만 적용됩니다.

- HA를 활성화하면 HA 진행이 Active(활성) 상태로 변경된 후 모든 경로가 강제로 삭제되고 다시 추가됩니다. 이 단계에서 연결이 손실될 수 있습니다.
- 관리 센터 또는 디바이스 관리자를 사용하여 위협 방어 고가용성을 생성하는 동안 선택한 보조 위협 방어 디바이스의 모든 기존 구성이 선택한 기본 위협 방어 디바이스에서 복제된 구성으로 바뀌므로 HA(고가용성) 생성 시 주 디바이스를 신중하게 선택합니다. 예를 들어 기존 기본 디바이스에 결함이 발생하여 RMA(Return Material Authorization)를 사용하여 HA를 교체한 경우 HA를 생성하는 동안 선택한 기본 디바이스의 모든 구성이 교체 디바이스로 복제되도록 보조 디바이스를 선택해야 합니다.
- 수백 개의 인터페이스가 구성된 HA의 Cisco Firepower 2100 및 1100 Threat Defense 디바이스를 구축하면 페일오버 시간(초)의 지연이 늘어날 수 있습니다.
- ASA 또는 Threat Defense HA 구성에서는 일반적으로 포트 53을 사용하는 수명이 짧은 연결은 빠르게 닫히고 액티브에서 스탠바이로 전송되거나 동기화되지 않습니다. 따라서 두 HA 디바이스의 연결 수에 차이가 있을 수 있습니다. 이는 수명이 짧은 연결의 정상적인 동작입니다. 수명이 긴 연결(예: 30~60초 이상)을 비교해볼 수 있습니다.

고가용성 쌍 추가

액티브/스탠바이 고가용성 쌍을 설정하는 경우 하나를 기본 디바이스로 지정하고 다른 하나를 보조 디바이스로 지정합니다. management center에서는 페어링된 디바이스에 병합된 설정을 구축합니다. 충돌이 있는 경우 기본 디바이스 설정이 사용됩니다.

다중 도메인 구축에서 고가용성 쌍의 디바이스는 동일한 도메인에 속해야 합니다.

참고 페일오버 링크 및 상태 저장 페일오버 링크는 프라이빗 IP 공간에 있으며 고가용성 쌍의 피어 간 통신에만 사용됩니다. 고가용성이 설정된 후에는 고가용성 쌍을 해제하고 재구성하지 않고는 선택한 인터페이스 링크 및 암호화 설정을 수정할 수 없습니다.

주의 고가용성 쌍을 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

시작하기 전에

두 디바이스에 대해 다음을 확인합니다.

- 같은 모델이어야 합니다.

- 인터페이스의 개수와 유형이 동일해야 합니다.
- 동일한 도메인 및 그룹에 포함되어야 합니다.
- 정상 상태이고 동일한 소프트웨어를 실행해야 합니다.
- 라우팅 또는 투명 모드가 필요합니다.
- NTP 구성이 같아야 합니다. 시간 동기화의 내용을 참조하십시오.
- 커밋되지 않은 변경 사항 없이 완전히 구축되어야 합니다.
- DHCP 또는 PPPoE가 인터페이스에 구성되어 있지 않아야 합니다.

참고 기본 디바이스에서 사용 가능한 인증서가 보조 디바이스에 존재하지 않는 경우, 두 개의 threat defense 디바이스 간 고가용성 구성이 가능합니다. 고가용성이 구성되면 보조 디바이스에 인증서가 동기화됩니다.

프로시저

단계 **1** Management Center에 디바이스 추가에 따라 management center에 두 디바이스를 추가합니다.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **3** **Add(**추가**)** 드롭다운 메뉴에서 **High Availability(**고가용성**)**을 선택합니다.

단계 **4** 고가용성 쌍에 대한 표시 **Name(**이름**)**을 입력합니다.

단계 **5** 장치 유형에서 **Firepower Threat Defense**를 선택합니다.

단계 **6** 고가용성 쌍에 **Primary Peer(**기본 피어**)** 디바이스를 선택합니다.

단계 **7** 고가용성 쌍에 **Secondary Peer(**보조 피어**)** 디바이스를 선택합니다.

단계 **8** **Continue(**계속**)**를 클릭합니다.

단계 **9** **LAN Failover Link(LAN** 페일오버 링크**)**에서 페일오버 통신이 충분히 가능한 대역폭이 있는 **Interface(**인터페이스**)**를 선택합니다.

참고 논리적 이름을 갖지 않고 보안 영역에 속하지 않은 인터페이스만 고가용성 쌍 추가 대화상자의 인터페이스 드롭다운 메뉴에 표시됩니다.

단계 **10** 식별된 논리적 이름을 입력합니다.

단계 **11** 액티브 유닛에서 페일오버 링크에 대한 기본 **IP** 주소를 입력합니다.

이 주소는 사용되지 않는 서브넷에 있어야 합니다. 이 서브넷은 두 개의 IP 주소만 사용하며 31비트(255.255.255.254 또는 /31)가 될 수 있습니다.

참고 169.254.1.0/24 및 fd00:0:0:*::/64 는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.

단계 **12** 필요에 따라 **IPv6** 주소 사용을선택합니다.

단계 **13** 스탠바이 유닛에서 페일오버 링크에 대한 보조 **IP** 주소를 입력합니다. 이 IP 주소는 기본 IP 주소와 동일한 서브넷에 있어야 합니다.

단계 **14** IPv4 주소를 사용하는 경우 기본 및 보조 IP 주소에 적용되는 서브넷 마스크 를 입력합니다.

단계 **15** 필요에 따라 **Stateful Failover Link(**스테이트풀 페일오버 링크**)**에서 동일한 **Interface(**인터페이스**)**를 선택하거나 다른 인터페이스를 선택하고 고가용성 구성 정보를 입력합니다.

이 서브넷은 두 개의 IP 주소만 사용하며 31비트(255.255.255.254 또는 /31)가 될 수 있습니다.

참고 169.254.1.0/24 및 fd00:0:0:*::/64 는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.

단계 **16** 필요에 따라 활성화를 선택하고 페일오버 링크 간 IPsec 암호화 용 키 생성 방법을 선택합니다.

단계 **17** **OK(**확인**)**를 클릭합니다. 이때 시스템에서 데이터를 동기화하는 데 몇 분 정도 걸립니다.

다음에 수행할 작업

디바이스를 백업합니다. 백업을 이용하면 장애가 발생한 디바이스를 빠르게 교체하고, management center와의 연결을 해제하지 않고도 고가용성 서비스를 복원할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드을 참조하십시오.

선택적 고가용성 파라미터 구성

management center에서 초기 고가용성 설정을 볼 수 있습니다. 고가용성 쌍을 해제하고 다시 설정하지 않으면 이러한 설정을 편집할 수 없습니다.

페일오버 결과를 개선하기 위해 페일오버 트리거 기준을 편집할 수 있습니다. 인터페이스 모니터링은 페일오버에 가장 적합한 인터페이스를 결정하도록 합니다.

스탠바이 IP 주소 및 인터페이스 모니터링 구성

각 인터페이스에 대한 스탠바이 IP 주소를 설정합니다. 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다.

기본적으로 모니터링은 모든 물리적 인터페이스에서 활성화되며, Firepower 1010에서는 논리적 이름이 구성된 모든 VLAN 인터페이스에서 활성화됩니다. 중요도가 낮은 네트워크에 연결된 인터페이스를 제외하여 페일오버 정책에 영향을 미치지 않도록 하고자 할 수 있습니다. Firepower 1010 스위치 포트는 인터페이스 모니터링에 적용되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **High Availability(**고가용성**)** 탭을 클릭합니다.

단계 **4** 모니터링되는 인터페이스 영역에서 편집하려는 인터페이스 옆의 **Edit(**수정**)** ( )를 클릭합니다.

단계 **5** 오류에 대해 이 인터페이스 모니터링 확인란을 선택합니다.

단계 **6** **IPv4** 탭에서 스탠바이 **IP** 주소를 입력합니다.

이 주소는 액티브 IP 주소와 같은 네트워크에 있는 여유 주소여야 합니다.

단계 **7** **IPv6** 탭에서 수동으로 IPv6 주소를 구성하는 경우 액티브 IP 주소 옆의 **Edit(**수정**)** ( )를 클릭하고 스탠바이 **IP** 주소를 입력한 뒤 **OK**를 클릭합니다.

이 주소는 액티브 IP 주소와 같은 네트워크에 있는 여유 주소여야 합니다. 자동으로 생성되거나 **EUI 64** 강제 적용된 주소의 경우 스탠바이 주소가 자동으로 생성됩니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

고가용성 페일오버 기준 수정

네트워크 구축에 따라 페일오버 기준을 사용자 정의할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** **Failover Trigger Criteria(**페일오버 트리거 기준**)** 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** **Interface Failure Threshold(**인터페이스 페일오버 임계값**)**에서 디바이스 페일오버 이전에 오류가 발생해야 하는 인터페이스의 수 또는 비율을 선택합니다.

단계 **6** **Hello** 패킷 간격**(Hello** 패킷 간격**)**에서 페일오버 링크에 보낼 Hello 패킷 수를 선택합니다.

참고 Firepower 2100에서 원격 액세스 VPN을 사용한다면, 기본 Hello 패킷 간격을 사용합니다. 그렇지 않으면 높은 CPU 사용량 때문에 페일오버가 발생할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

가상 MAC 주소 구성

Secure Firewall Management Center의 두 위치에서 페일오버에 대해 액티브 및 스탠바이 MAC 주소를 구성할 수 있습니다.

- 인터페이스 구성 중 인터페이스 편집 내 고급 탭에 대한 설명은 MAC 주소 구성의 내용을 참조하십시오.
- 고가용성 페이지에서 액세스한 인터페이스 MAC 주소 추가는 이 절차를 참고하십시오.

참고 기본 유닛과 보조 유닛 모두에서 MAC 주소를 구성하려면(MAC 주소가 두 HA 유닛의 모든 하위 인터페이스로 전송되도록) **Interfaces(**인터페이스**)** 탭을 사용하여 액티브 및 스탠바이 HA 유닛 모두에 걸쳐 하위 인터페이스의 MAC 주소를 복제하는 것이 좋습니다.

액티브 및 스탠바이 MAC 주소가 두 위치에 구성되면 페일오버 시 인터페이스 구성 중 설정한 주소가 우선됩니다.

물리적 인터페이스에 액티브 및 스탠바이 MAC 주소를 지정하여 페일오버 중 트래픽 손실을 최소화할 수 있습니다. 이 기능은 페일오버에 대한 IP 주소 매핑의 이중화를 제공합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 인터페이스 MAC 주소 옆의 **Add(**추가**)** ( )을 선택합니다.

단계 **5** 물리적 인터페이스를 선택합니다.

단계 **6** 액티브 인터페이스 **MAC** 주소를 입력합니다.

단계 **7** 스탠바이 인터페이스 **MAC** 주소를 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

고가용성 관리

이 섹션에서는 고가용성를 활성화한 다음, 고가용성 유닛을 관리하는 방법을 설명합니다. 고가용성 설정을 변경하고 한 유닛에서 다른 유닛으로의 장애 조치를 강제로 수행하는 방법도 알아봅니다.

Threat Defense 고가용성 쌍에서 활성 피어 전환

threat defense 고가용성 쌍을 설정하면 액티브 및 스탠바이 유닛을 수동으로 전환할 수 있으며 현재 액티브 유닛의 영구 오류 또는 상태 이벤트 시 페일오버를 효과적으로 강제할 수 있습니다. 이 절차를 완료하기 전 두 유닛이 모두 완전히 구축되어야 합니다.

시작하기 전에

단일 Threat Defense 고가용성 쌍의 노드 상태 새로 고침 , 25 페이지. 이렇게 하면 threat defense 고가용성 쌍 상태에서는 management center의 상태가 동기화됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 액티브 피어를 변경할 고가용성 쌍 옆에 있는 **Switch Active Peer(**액티브 피어 전환**)**를 클릭합니다.

단계 **3** 다음 작업을 수행할 수 있습니다.

- **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.
- 취소하고 디바이스 관리 페이지로 돌아가려면 아니오를 클릭합니다.

단일 Threat Defense 고가용성 쌍의 노드 상태 새로 고침

threat defense 고가용성 쌍의 액티브 또는 스탠바이 디바이스가 재부팅될 때마다 management center은 정확한 고가용성 상태를 표시하지 않을 수 있습니다. 이는 디바이스가 재부팅될 때 고가용성 상태가 즉시 디바이스에 업데이트되고 해당 이벤트가 management center에 전송되기 때문입니다. 그러나 디바이스와 management center의 통신이 아직 설정 전이기 때문에 상태는 management center에 업데이트 되지 않습니다.

management center와 디바이스 간 통신 실패 또는 약한 통신 채널은 데이터 동기화 오류를 발생시킬 수 있습니다. 고가용성 쌍 내에서 액티브 및 스탠바이 디바이스를 전환하는 경우 상당한 시간이 지난 뒤에도 해당 변경 사항이 management center에 반영되지 않을 수 있습니다.

이 경우 고가용성 노드 상태를 새로 고침하여 고가용성 쌍의 액티브 및 스탠바이 디바이스의 정확한 정보를 얻을 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 노드 상태를 새로 고침 하려는 고가용성 쌍 옆의 **HA** 노드 상태 새로 고침을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 노드 상태를 새로 고칩니다.

고가용성 일시 중단 또는 재개

고가용성 쌍의 유닛을 일시 중단할 수 있습니다. 이는 다음과 같은 경우에 유용합니다.

- 두 유닛이 모두 액티브-액티브인 상태에서 페일오버 링크의 통신을 수정해도 문제가 해결되지 않는 경우.
- 액티브 또는 스탠바이 유닛을 트러블슈팅하고 트러블슈팅 중에는 유닛을 페일오버하지 않으려는 경우.

고가용성을 일시 중단할 경우 현재 액티브 디바이스는 액티브 상태로 유지되어 모든 사용자 연결을 처리합니다. 그러나 페일오버 기준은 더 이상 모니터링되지 않으며 시스템은 현재 의사 스탠바이 디바이스로 페일오버되지 않습니다.

고가용성 일시 중단과 고가용성 해제의 주요 차이점은 일시 중단된 고가용성 디바이스에서는 고가용성 구성이 보존된다는 것입니다. 반면 고가용성을 해제하면 구성이 지워집니다. 따라서 일시 중단된 시스템에서 고가용성을 다시 시작하는 옵션이 제공됩니다. 그러면 기존 구성이 활성화되며 두 디바이스가 다시 페일오버 쌍으로 작동합니다.

고가용성을 일시 중단하려면 **configure high-availability suspend** 명령을 사용합니다.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

액티브 유닛에서 고가용성을 일시 중단하면 액티브 유닛과 스탠바이 유닛 둘 다에서 구성이 일시 중단됩니다. 스탠바이 유닛 인터페이스 구성도 지워집니다. 스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 스탠바이 유닛에서만 고가용성이 일시 중단되며 액티브 유닛은 일시 중단된 유닛으로의 페일오버를 시도하지 않습니다.

페일오버를 재시작하려면 **configure high-availability resume** 명령을 사용합니다.

```
> configure high-availability resume
Successfully resumed high-availablity.
```

Suspended(일시 중단됨) 상태인 유닛만 다시 시작할 수 있습니다. 이 유닛은 피어 유닛과 액티브/스탠바이 상태를 협상합니다.

참고 고가용성 일시 중단은 임시 상태입니다. 유닛을 다시 불러오면 고가용성 구성을 자동으로 재시작하고 피어와 액티브/스탠바이 상태 협상을 시작합니다.

Threat Defense 고가용성 쌍의 유닛 교체

백업 파일을 사용하여 threat defense 고가용성 쌍에서 장애가 발생한 유닛을 교체하려면 Cisco Secure Firewall Management Center 관리 가이드의 *Management Center* 및 매니지드 디바이스 복원을 참조하십시오.

장애가 발생한 디바이스의 백업이 없는 경우 고가용성을 해제해야 합니다. 그런 다음 Secure Firewall Management Center에 교체 디바이스를 등록하고 고가용성을 다시 설정합니다. 이 프로세스는 디바이스가 기본 디바이스인지 보조 디바이스인지에 따라 달라집니다.

- 기본 Threat Defense HA 유닛을 백업 없이 교체, 27 페이지
- 보조 Threat Defense HA 유닛을 백업 없이 교체, 28 페이지

기본 Threat Defense HA 유닛을 백업 없이 교체

threat defense 고가용성 쌍에서 장애가 발생한 기본 유닛을 교체하려면 다음 단계를 수행합니다. 다음 단계를 수행하지 않으면 기존 고가용성 설정을 오버라이트할 수 있습니다.

주의 threat defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

주의 디스크를 이미지 재설치하지 않고 센서 또는 management center에서 다른 디바이스로 디스크를 이동하지 마십시오. 이는 지원되지 않는 구성이므로 기능이 중단될 수 있습니다.

프로시저

단계 **1** 고가용성 쌍을 분리하기 위해 강제 해제를 선택합니다. 고가용성 쌍 분리, 28 페이지를 참조하십시오.

참고 중단 작업은 threat defense 및 management center에서 HA와 관련된 모든 구성을 제거하며, 나중에 수동으로 다시 생성해야 합니다. 동일한 HA 쌍을 설정하려면 HA 중단 작업을 실행하기 전에 모든 인터페이스/하위 인터페이스의 IP, MAC 주소, 모니터링 설정을 저장해야 합니다.

단계 **2** management center에서 오류가 발생한 기본 threat defense 디바이스의 등록을 해제하려면 Management Center에서 디바이스 삭제(등록 해제)의 내용을 참조하십시오.

단계 **3** management center에 threat defense의 교체 디바이스를 등록합니다. Management Center에 디바이스 추가의 내용을 참조하십시오.

단계 **4** 등록 시 기존 보조/액티브 유닛을 기본 디바이스로 사용하고 교체 디바이스를 보조/스탠바이 디바이스로 하여 고가용성을 구성하려면 고가용성 쌍 추가, 20 페이지을 참조하십시오.

보조 **Threat Defense HA** 유닛을 백업 없이 교체

threat defense 고가용성 쌍에서 장애가 발생한 보조 유닛을 교체하려면 다음 단계를 수행합니다.

⚠

주의 threat defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

프로시저

단계 **1** 고가용성 쌍을 분리하기 위해 강제 해제를 선택합니다. 고가용성 쌍 분리, 28 페이지를 참조하십시오.

참고 중단 작업은 threat defense 및 management center에서 HA와 관련된 모든 구성을 제거하며, 나중에 수동으로 다시 생성해야 합니다. 동일한 HA 쌍을 설정하려면 HA 중단 작업을 실행하기 전에 모든 인터페이스/하위 인터페이스의 IP, MAC 주소, 모니터링 설정을 저장해야 합니다.

단계 **2** management center에서 보조 threat defense디바이스의 등록을 해제합니다. Management Center에서 디바이스 삭제(등록 해제)의 내용을 참조하십시오.

단계 **3** management center에 threat defense의 교체 디바이스를 등록합니다. Management Center에 디바이스 추가의 내용을 참조하십시오.

단계 **4** 등록 시 기존 기본/액티브 유닛을 기본 디바이스로 사용하고 교체 디바이스를 보조/스탠바이 디바이스로 하여 고가용성을 구성하려면 고가용성 쌍 추가, 20 페이지을 참조하십시오.

고가용성 쌍 분리

고가용성 쌍을 분리하면 고가용성 구성이 두 유닛에서 모두 제거됩니다.

액티브 유닛은 가동 상태를 유지하며 트래픽을 전달합니다. 스탠바이 유닛 인터페이스 구성이 지워집니다.

분리 작업이 진행되기 전 액티브 유닛에 구축되지 않은 정책은 분리 작업이 완료된 뒤에도 구축되지 않습니다. 분리 작업이 완료되면 독립형 디바이스의 정책을 구축합니다.

참고 management center를 사용하여 고가용성 쌍에 연결할 수 없는 경우 각 디바이스에서 CLI에 연결하고 **configure high-availability disable**을 입력하여 수동으로 고가용성을 해제합니다. 고가용성 쌍을 삭제(등록 해제)하고 새 Management Center에 등록, 30 페이지도 참조하십시오.

주의 threat defense 고가용성 쌍을 분리하면 기본 및 보조 유닛에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오.

Threat Defense 기능 기록**:**

- 7.2 - 이제 고가용성 쌍을 등록 해제하는 경우 고가용성 쌍을 분리하지 않고 재등록할 수 있습니다.

시작하기 전에

- 단일 Threat Defense 고가용성 쌍의 노드 상태 새로 고침 , 25 페이지. 이렇게 하면 고가용성 쌍 상태에서는 management center의 상태가 동기화됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 분리하려는 고가용성 쌍 옆의 **Break HA(HA** 분리**)**를 클릭합니다.

단계 **3** 스탠바이 피어가 응답하지 않으면 **Force Break(**강제 분리**)**를 선택합니다.

단계 **4** **Yes(**예**)**를 클릭합니다. 고가용성 쌍이 분리됩니다.

분리 작업은 액티브 및 스탠바이 유닛에서 고가용성 구성을 제거합니다.

액티브 유닛에 구축된 FlexConfig 정책은 고가용성 해제 작업 완료 후 구축 실패를 표시할 수 있습니다. FlexConfig 정책을 변경하고 액티브 유닛에 다시 구축해야 합니다.

다음에 수행할 작업

액티브 유닛에서 FlexConfig 정책을 사용하는 경우 구축 오류를 제거하기 위해 FlexConfig 정책을 변경하고 다시 구축합니다.

고가용성 쌍을 삭제(등록 해제)하고 새 **Management Center**에 등록

management center에서 고가용성 쌍을 등록 해제할 수 있습니다. 그래도 고가용성 쌍은 그대로 유지됩니다. 새 management center에 고가용성 쌍을 등록하려고 하거나 management center에서 더 이상 고가용성 쌍에 연결할 수 없는 경우, 해당 쌍을 등록 해제할 수 있습니다.

고가용성 쌍 등록 해제:

- management center와 고가용성 쌍 간의 모든 통신이 단절됩니다.
- **Device Management(**디바이스 관리**)** 페이지에서 해당 쌍을 제거합니다.
- 고가용성 쌍이 NTP를 사용하여 management center에서 시간을 수신하도록 클러스터의 플랫폼 설정 정책이 구성된 경우 해당 쌍을 로컬 시간 관리로 되돌립니다.
- 구성을 그대로 유지하므로 고가용성 쌍이 트래픽을 계속 처리합니다.

  NAT 및 VPN, ACL 및 인터페이스 구성과 같은 정책은 그대로 유지됩니다.

고가용성 쌍을 동일하거나 다른 management center에 다시 등록하면 설정이 제거되므로 해당 쌍은 이 시점에서 트래픽 처리를 중지합니다. 고가용성 구성은 그대로 유지되므로 쌍 전체를 추가할 수 있습니다. 등록 시 액세스 제어 정책을 선택할 수 있지만, 등록 후에 다른 정책을 다시 적용하고 구성을 구축해야만 트래픽을 다시 처리할 수 있습니다.

시작하기 전에

- 이 절차에서는 기본 유닛에 대한 CLI 액세스가 필요합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 등록을 해제하려는 고가용성 쌍 옆의 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭합니다. 디바이스 고가용성 쌍의 등록이 취소됩니다.

단계 **4** 기본 유닛을 새 디바이스로 추가하여 고가용성 쌍을 새(또는 동일한) management center에 등록할 수 있습니다.

a) 한 유닛에서 CLI에 연결하고 **show failover** 명령을 입력하여 기본 유닛을 확인합니다.

출력의 첫 번째 행에는 이 유닛이 Primary(기본)인지 아니면 Secondary(보조)인지가 표시됩니다.

```
> show failover
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On

[...]
```

b) 기본 유닛의 CLI에서 **configure manager add** 명령을 사용해 새 management center를 식별합니다. CLI에서 Threat Defense 관리 인터페이스 수정의 내용을 참조하십시오.

c) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택한 다음 **Add Device(**디바이스 추가**)**를 클릭합니다.

기본 유닛을 디바이스로 추가하기만 하면 management center가 보조 유닛을 검색합니다.

모니터링 고가용성

이 섹션에서는 고가용성 상태를 모니터링할 수 있습니다.

페일오버 기록 보기

두 개의 고가용성 디바이스의 페일오버를 단일 보기에서 볼 수 있습니다. 시간 순으로 표시되며 페일오버의 이유를 표시합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 요약을 선택합니다.

단계 **4** General(일반)에서 **View(**보기**)** ( )을 클릭합니다.

스테이트풀 페일오버 통계 보기

고가용성 쌍의 기본 및 보조 디바이스에 대한 스테이트풀 고가용성 링크 통계를 볼 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** Stateful Failover Link(스테이트풀 페일오버 링크)에서 **View(**보기**)** ( )를 클릭합니다.
단계 **5** 통계를 보려는 디바이스를 선택합니다.

고가용성 기록

기능	버전	세부정보
이제 고가용성 쌍을 등록 해제하는 경우 고가용성 쌍을 해제하지 않고 재등록할 수 있습니다.	7.3	고가용성 쌍을 삭제(등록 해제)하는 경우 CLI에서 수동으로 고가용성을 해제하고 독립형 디바이스를 재등록할 필요가 없습니다. 이제 기본 유닛을 새 management center에 추가할 수 있습니다. 그러면 스탠바이 유닛이 자동으로 검색됩니다. 고가용성 쌍을 재등록해도 구성이 지워지며 정책을 다시 적용해야 합니다.
고가용성을 위한 정책 롤백 지원	7.2	**configure policy rollback** 명령은 고가용성을 위해 지원됩니다.
더 빠른 HA 피어링을 위한 구성 동기화 최적화 기능	7.2	구성 동기화 최적화 기능을 사용하면 구성 해시 값을 교환하여 조인 유닛과 액티브 유닛의 구성을 비교할 수 있습니다. 액티브 유닛과 조인 유닛 모두에서 계산된 해시가 일치하는 경우, 조인 유닛은 전체 config-sync를 건너뛰고 HA에 다시 조인합니다. 이 기능을 사용하면 HA 피어링 속도가 빨라지고 유지 관리 기간과 업그레이드 시간이 단축됩니다.
클러스터링된 디바이스 및 고가용성 디바이스에 대한 업그레이드 워크플로우 개선	7.1	클러스터링된 디바이스 및 고가용성 디바이스에 대한 업그레이드 워크플로우가 다음과 같이 개선되었습니다. • 이제 업그레이드 마법사에서 클러스터링된 고가용성 유닛을 개별 디바이스가 아닌 그룹으로 올바르게 표시합니다. 시스템은 사용자에게 발생할 수 있는 그룹 관련 문제를 식별하고, 보고하고, 사전에 수정을 요구할 수 있습니다. 예를 들어 Firepower Chassis Manager에서 동기화되지 않은 변경 사항을 적용한 경우 Firepower 4100/9300에서 클러스터를 업그레이드할 수 없습니다. • 업그레이드 패키지를 클러스터 및 고가용성 쌍으로 복사하는 속도와 효율성을 개선했습니다. 이전에는 FMC에서 패키지를 각 그룹 멤버에 순차적으로 복사했습니다. 이제 그룹 멤버는 일반 동기화 프로세스의 일부로 서로 패키지를 가져올 수 있습니다. • 이제 클러스터에서 데이터 유닛의 업그레이드 순서를 지정할 수 있습니다. 제어 유닛은 항상 마지막에 업그레이드됩니다.
고가용성 그룹 또는 클러스터에서 경로 지우기.	7.1	이전 릴리스에서 **clear route** 명령은 유닛에서만 라우팅 테이블을 지웠습니다. 이제 고가용성 그룹 또는 클러스터에서 작동하는 경우 이 명령은 액티브 또는 제어 유닛에서만 사용할 수 있으며, 그룹 또는 클러스터의 모든 유닛에서 라우팅 테이블을 지웁니다.

기능	버전	세부정보

FTD 고가용성 강화	6.2.3	6.2.3 버전에는 고가용성 상태의 FTD 디바이스를 위해 다음과 같은 기능이 도입되었습니다.
		• 고가용성 쌍의 액티브 또는 스탠바이 FTD 디바이스가 재시작될 때마다 FMC는 매니지드 디바이스에 대해 정확한 고가용성 상태를 표시하지 않을 수 있습니다. 그러나 디바이스와 FMC의 통신이 아직 설정 전이기 때문에 상태는 FMC에서 업그레이드되지 않을 수 있습니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지의 **Refresh Node Status(**노드 상태 새로 고침**)** 옵션을 통해 고가용성 유닛 상태를 새로 고쳐 고가용성 쌍의 액티브 및 스탠바이 디바이스에 대한 정확한 정보를 얻을 수 있습니다.
		• FMC UI의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에 새로운 **Switch Active Peer(**액티브 피어 전환**)** 아이콘이 도입되었습니다.
		• 버전 6.2.3에는 새로운 REST API 개체인 디바이스 고가용성 쌍 서비스가 포함되어 있으며, 여기에는 4가지 기능이 있습니다.
		  • **DELETE ftddevicehapairs**
		  • **PUT ftddevicehapairs**
		  • **POST ftddevicehapairs**
		  • **GET ftddevicehapairs**