



고가용성

다음 주제에서는 Cisco Secure Firewall Management Center의 액티브/스탠바이 고가용성 구성 방법을 설명합니다.

- [Management Center 고가용성 정보, 1 페이지](#)
- [Firepower Management Center 고가용성을 위한 요구 사항, 8 페이지](#)
- [Management Center 고가용성의 전제조건, 11 페이지](#)
- [Management Center 고가용성 설정, 11 페이지](#)
- [Management Center 고가용성 상태 보기, 13 페이지](#)
- [Management Center 고가용성 쌍에서 동기화된 구성, 14 페이지](#)
- [고가용성 쌍의 Management Center 데이터베이스에 대한 외부 액세스 구성, 15 페이지](#)
- [Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인, 15 페이지](#)
- [Management Center 고가용성 쌍에서 피어 전환, 16 페이지](#)
- [쌍을 이룬 Management Center 간에 통신 일시 중지, 16 페이지](#)
- [쌍을 이룬 Management Center 간에 통신 다시 시작, 17 페이지](#)
- [고가용성 쌍의 Management Center IP 주소 변경, 17 페이지](#)
- [Management Center 고가용성 비활성화, 18 페이지](#)
- [고가용성 쌍의 Management Center 교체, 18 페이지](#)
- [고가용성 쌍의 Management Center 복원\(하드웨어 장애 없음\), 23 페이지](#)
- [Management Center 고가용성 히스토리, 25 페이지](#)

Management Center 고가용성 정보

운영의 연속성을 보장하려면 고가용성 기능을 사용하여 디바이스 관리를 위한 이중 management center를 지정할 수 있습니다. management center는 하나의 어플라이언스가 액티브 유닛이며 디바이스를 관리하는 액티브/스탠바이 고가용성을 지원합니다. 스탠바이 유닛은 디바이스를 활동적으로 관리하지 않습니다. 액티브 유닛은 구성 데이터를 데이터 저장소로 기록하고 두 유닛 모두에 대해 데이터를 복제하며 필요한 경우 동기화를 사용하여 스탠바이 유닛과 정보를 공유합니다.

Active/Standby(액티브/스탠바이) 고가용성을 사용하면 보조 management center를 구성하고 장애가 발생한 경우 기본 management center의 기능을 대체합니다. 기본 management center에 장애가 발생하는 경우 보조 management center를 승격하여 액티브 유닛으로 만들 수 있습니다.

이벤트 데이터는 매니지드 디바이스에서 고가용성 쌍에 있는 management center 모두로 흐릅니다. 한 management center가 실패하면 다른 management center를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다.

참고로 고가용성 쌍으로 구성된 management center는 신뢰할 수 있는 동일한 관리 네트워크에 있어야 할 필요가 없으며 동일한 지리적 위치에 있어야 할 필요도 없습니다.



주의 시스템이 일부 기능을 액티브 management center로 제한하므로 해당 어플라이언스가 실패하면 스탠바이 management center를 액티브로 승격해야 합니다.



참고 변경 구축에 성공한 직후 management center에서 전환을 트리거하면 새 액티브 management center에서 미리보기 구성이 작동하지 않을 수 있습니다. 이는 정책 구축 기능에 영향을 주지 않습니다. 필요한 동기화가 완료된 후 management center에서 전환을 트리거하는 것이 좋습니다.

마찬가지로, management center HA 동기화 상태가 저하된 상태에서 전환을 트리거하거나 역할을 변경하면 management center HA가 데이터베이스를 손상시키고 심각한 상황을 초래할 수 있습니다. 이 문제를 해결하기 위해 추가 지원이 필요하다면 Cisco TAC(Technical Assistance Center)에 즉시 문의하는 것이 좋습니다.

이 HA 동기화는 여러 가지 이유로 성능이 저하된 상태로 끝날 수 있습니다. 이 장의 [고가용성 쌍의 Management Center 교체, 18 페이지](#) 섹션에서는 일부 실패 시나리오와 문제를 해결하는 후속 절차를 다룹니다. 성능 저하의 이유 또는 시나리오가 설명된 시나리오와 일치하는 경우 다음 단계에 따라 문제를 해결합니다. 다른 작업은 TAC에 문의하는 것이 좋습니다.

원격 액세스 **VPN** 고가용성에 대한 정보

기본 디바이스에 Remote Access(원격 액세스) VPN 구성과 CertEnrollment 개체로 등록된 ID 인증서가 있는 경우, 보조 디바이스에 동일한 CertEnrollment 개체로 등록된 ID 인증서가 있어야 합니다. CertEnrollment 개체는 디바이스별 재정의로 인해 기본 및 보조 디바이스에 대해 서로 다른 값을 가질 수 있습니다. 고가용성 형성 하기 전에 두 개의 디바이스를 등록 하는 동일한 CertEnrollment 개체에 한 개로 제한이 됩니다.

Management Center 고가용성에서의 **SNMP** 동작

SNMP 구성 HA 쌍에서 알림 정책을 구축하면 기본 management center가 SNMP 트랩을 전송합니다. 기본 management center에 오류가 발생하면 액티브 유닛이 되는 보조 management center는 추가 구성 없이 SNMP 트랩을 전송합니다.

Firepower Management Center 고가용성의 역할 및 상태 비교

기본/보조 역할

Secure Firewall Management Center의 고가용성 쌍을 설정할 때 한 Secure Firewall Management Center를 기본, 다른 하나를 보조로 구성합니다. 컨피그레이션 중에는 기본 유닛의 정책이 보조 유닛에 동

기화됩니다. 동기화가 끝나면 기본 Secure Firewall Management Center은 액티브 피어가 되고 보조 Secure Firewall Management Center는 보조 피어로 두 유닛이 매니지드 디바이스 및 정책 설정에 단일 어플라이언스로 작동합니다.

액티브/스탠바이 상태

고가용성 쌍에서 두 Secure Firewall Management Center의 가장 큰 차이는 액티브 및 스탠바이 피어와 관련이 있습니다. 액티브 Secure Firewall Management Center는 모든 기능을 사용할 수 있으며 디바이스와 정책을 관리할 수 있습니다. 스탠바이 Secure Firewall Management Center는 기능이 숨겨져 있으며 설정 변경을 할 수 없습니다.

Management Center 고가용성 쌍의 이벤트 처리

고가용성 쌍의 두 management center가 관리된 디바이스에서 이벤트를 수신하므로 어플라이언스용 관리 IP 주소를 공유하지 않습니다. 즉 management center 중 하나에 오류가 발생하는 경우 이벤트를 지속적으로 처리하기 위해 개입할 필요가 없습니다.

AMP 클라우드 연결 및 악성코드 정보

이들은 파일 정책 및 관련 컨피그레이션을 공유하지만 고가용성 쌍의 management center과 Cisco AMP Cloud 연결과 악성코드 성향을 공유하지 않습니다. 운영 연속성을 보장하고 탐지된 파일의 악성코드 속성이 두 management center 및 기본과 보조 management center에 동일하려면 AMP 클라우드에 대한 액세스 권한이 있어야 합니다.

URL 필터링 및 보안 인텔리전스

URL 필터링과 보안 인텔리전스의 설정 및 정보는 고가용성 구축에서 Secure Firewall Management Center 간에 동기화됩니다. 그러나 기본 Secure Firewall Management Center만 URL 카테고리 및 평판 데이터 그리고 보안 인텔리전스 피드에 대한 업데이트를 다운로드합니다.

기본 Secure Firewall Management Center에 장애가 발생하면 위협 인텔리전스 데이터 업데이트를 위해 보조 Secure Firewall Management Center가 인터넷에 액세스할 수 있는지 확인하고 보조 Secure Firewall Management Center의 웹 인터페이스를 사용해 액티브로 전환합니다.

Management Center 페일오버 중에 사용자 데이터 처리

기본 management center에 장애가 발생하면 보조 management center가 TS Agent ID 소스 소스에서 관리되는 디바이스 사용자 - IP 매핑을 전파하고, ISE / ISE-PIC ID 소스에서 SGT 매핑을 전파합니다. ID 소스로 아직 확인되지 않은 사용자는 알 수 없음으로 식별됩니다.

다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.

Management Center 고가용성 쌍에서 구성 관리

고가용성 구축에서 액티브 management center만 디바이스를 관리하고 정책을 적용할 수 있습니다. 두 management center 모두 지속적인 동기화 상태를 유지합니다.

액티브 management center에 오류가 발생하는 경우 고가용성 쌍은 사용자가 수동으로 스탠바이 어플라이언스를 액티브 상태로 승격할 때까지 저하 상태에 돌입합니다. 승격이 완료되면 어플라이언스는 유지 관리 모드 상태가 됩니다.

Management Center 고가용성 재해 복구

재해 복구 상황에서는 수동 전환을 수행해야 합니다. 기본 management center - FMC1에 오류가 발생하면 보조 management center인 FMC2의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 이는 보조(FMC2)에 장애가 발생하는 경우에도 반대로 적용됩니다. 자세한 내용은 [Management Center 고가용성 쌍에서 피어 전환, 16 페이지](#)를 참고하십시오.

실패한 management center 복원에 대해서는 [고가용성 쌍의 Management Center 교체, 18 페이지](#)의 내용을 참조하십시오.

SSO 및 고가용성 쌍

Management Center고가용성 설정의 FMC는 SSO(Single Sign-On, 단일 인증)를 지원할 수 있지만, 다음 사항을 고려해야 합니다.

- SSO 설정은 고가용성 쌍의 멤버 간에 동기화되지 않습니다. 쌍의 각 멤버에서 SSO를 별도로 설정해야 합니다.
- 고가용성 쌍의 두 management center는 모두 SSO에 동일한 ID 공급자(IdP)를 사용해야 합니다. SSO에 대해 설정된 각 management center의 IdP에서 서비스 제공자 애플리케이션을 설정해야 합니다.
- 둘 다 SSO를 지원하도록 설정된 management center 고가용성 쌍에서는 사용자가 SSO를 사용하여 보조 management center에 처음으로 액세스하기 전에 먼저 사용자가 SSO를 통해 기본 management center에 한 번 이상 로그인해야 합니다.
- 고가용성 쌍에서 management center에 대해 SSO를 설정하는 경우:
 - 기본 management center에서 SSO를 설정하는 경우, 보조 management center에서 SSO를 설정할 필요가 없습니다.
 - 보조 management center에서 SSO를 설정하는 경우, 기본 management center에서도 SSO를 설정해야 합니다. (SSO 사용자는 보조 management center에 로그인하기 전에 기본 management center에 한 번 이상 로그인해야 하기 때문입니다.)

관련 항목

[SAML SSO\(Single Sign-On\) 구성](#)

Management Center 백업 중에 고가용성 동작

management center 고가용성 쌍에서 백업을 수행할 경우 백업 작업은 피어 간 동기화를 일시 중지합니다. 이 작업을 수행하는 동안 액티브 management center를 계속 사용할 수 있지만 스탠바이 피어는 사용할 수 없습니다.

백업이 완료되면 동기화가 재시작되어 액티브 피어의 프로세스를 일시적으로 비활성화합니다. 이 일시 중지 상태에 고가용성 페이지는 모든 프로세스가 다시 시작될 때까지 일시적으로 보류 페이지를 표시합니다.

Management Center 고가용성 스플릿 브레인

고가용성 쌍에서 액티브 management center이 중단(전원 문제, 네트워크/연결 문제)되는 경우 스탠바이 management center를 액티브 상태로 승격시킵니다. 원래 액티브 피어가 복구되면 두 피어 모두 액티브 상태로 간주할 수 있습니다. 이 상태를 '스플릿 브레인' 상태라고 합니다. 이러한 상황이 발생하면 시스템은 액티브 어플라이언스를 선택하고 다른 어플라이언스를 스탠바이로 전환하도록 합니다.

액티브 management center이 중단(또는 네트워크 오류로 연결 끊기)되는 경우 고가용성 또는 스위치 역할을 중단할 수 있습니다. 스탠바이 management center는 성능 저하 상태에 진입합니다.



참고 스플릿 브레인을 해결하면 보조로 사용하는 어플라이언스의 모든 디바이스 등록 및 정책 설정이 손실됩니다. 예를 들어 보조에 존재하던 정책 수정 내용을 전부 잃지만 기본에 있던 것은 보존됩니다. management center이 두 어플라이언스가 액티브 상태인 고가용성 스플릿 브레인 시나리오에 돌입하고 스플릿 브레인을 해소하기 전에 관리되는 디바이스를 등록하고 정책을 구축하는 경우 모든 정책을 내보내고 관리되는 디바이스를 새 고가용성이 재구성되기 전에 해당 스탠바이 management center에서 등록 해제해야 합니다. 그런 다음 액티브 management center에서 관리되는 디바이스를 등록하고 정책을 가져올 수 있습니다.

고가용성 쌍에서 Management Center 업그레이드

Cisco는 온라인으로 다양한 유형의 업데이트를 주기적으로 배포합니다. 시스템 소프트웨어의 주요 및 사소한 업그레이드를 포함합니다. 고가용성 설정에서 management center에 이런 업데이트를 설치해야 할 수 있습니다.



경고! 업그레이드 중 하나 이상의 운영 management center이 있는지 확인하십시오.

시작하기 전에

업그레이드와 함께 배포된 릴리스 노트 또는 권고 사항을 읽습니다. 릴리스 정보에는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보가 제공됩니다.

프로시저

단계 1 액티브 management center의 웹 인터페이스에 액세스하고 데이터 동기화를 중단시키려면 [쌍을 이룬 Management Center 간에 통신 일시 중지](#), 16 페이지를 참조하십시오.

단계 2 스탠바이 management center을 업그레이드합니다.

업그레이드가 완료되면 스탠바이 유닛이 액티브상태가 됩니다. 두 피어가 액티브인 경우 고가용성 쌍은 저하(스플릿 브레인) 상태가 됩니다.

단계 3 다른 management center을 업그레이드합니다.

단계 4 어떤 management center을 스탠바이로 사용할지 결정합니다. 동기화가 중지된 뒤 스탠바이에 추가된 모든 추가 장치 또는 정책은 액티브 management center에 동기화되지 않습니다. 이러한 추가 디바이스만 등록을 취소하고 유지하려는 설정을 내보냅니다.

새 액티브 management center을 선택한 경우 보조로 지정한 management center는 디바이스 등록 및 동기화되지 않은 정책 설정 구축을 잃게 됩니다.

단계 5 정책 및 디바이스의 최신 요구 설정이 있는 새 액티브 management center을 선택하여 스플릿 브레인을 해결합니다.

Management Center 고가용성 문제 해결

이 섹션에서는 management center 고가용성 운영 오류에 대한 일반적인 정보를 설명합니다.

오류	설명	해결책
스탠바이에 로그인 하려면 먼저 활성 management center에서 비밀번호를 재설정해야 합니다.	계정에 강제 비밀번호 재설정이 활성화된 상태에서 대기 management center에 로그인하려 했습니다.	데이터베이스가 대기 management center에 대해 읽기 전용이므로, 액티브 management center의 로그인 페이지에서 비밀번호를 재설정해야 합니다.
500 내부	피어 역할 전환이나 동기화 중지 또는 재개 등 중요한 management center 고가용성 작업을 수행하는 동안 웹 인터페이스 접속을 시도할 때 표시될 수 있습니다.	작업이 완료되기를 기다린 뒤 웹 인터페이스를 사용합니다.

오류	설명	해결책
<p>시스템 프로세스가 시작 중이니 기다려 주시기 바랍니다.</p> <p>웹 인터페이스가 응답하지 않을 수 있습니다.</p>	<p>이는 고가용성 또는 데이터 동기화 중 management center이 재부팅될 때(수동 또는 전원 복구 중) 표시될 수 있습니다.</p>	<ol style="list-style-type: none"> 1. management center 셸에 액세스하여 <code>manage_hadc.pl</code> 명령을 사용해 management center 고가용성 구성 유틸리티에 액세스합니다. 참고 <code>sudo</code>를 사용하여 루트 사용자로 유틸리티를 실행합니다. 2. 옵션 5를 사용하여 미러링 작업을 일시 중지합니다. management center 웹 인터페이스를 재로딩합니다. 3. 웹 인터페이스를 사용하여 동기화를 다시 시작합니다. Integration(통합) > Other Integrations(기타 통합)를 선택한 다음, High Availability(고가용성) 탭을 클릭하고 Resume Synchronization(재시작 동기화)을 선택합니다.
<p>디바이스 등록 상태:호스트 <string> 연결할 수 없음</p>	<p>threat defense의 초기 구성 중에 management center IP 주소 및 NAT ID가 지정된 경우 Host(호스트) 필드를 비워둘 수 있습니다. 그러나 NAT 뒤에 management center가 모두 있는 HA 환경에서는 보조 management center에 threat defense를 추가하면 이 오류가 발생합니다.</p>	<ol style="list-style-type: none"> 1. 기본 management center에서 threat defense을 삭제합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 Management Center에서 디바이스 삭제를 참조하십시오. 2. <code>configure manager delete</code> 명령을 사용하여 threat defense에서 관리자를 제거합니다. Cisco Secure Firewall Threat Defense 명령 참조을 참조하십시오. 3. Host(호스트) 필드에 threat defense 디바이스의 IP 주소와 함께 management center에 threat defense를 추가합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 Management Center에 디바이스 추가를 참조하십시오.

오류	설명	해결책
디바이스 등록 상태: 호스트 <string> 연결할 수 없음	보조 management center 및 threat defense 디바이스가 모두 NAT 뒤에 있는 고가용성 구축에서 보조 management center 센터에 threat defense 디바이스를 추가하면 오류가 발생합니다.	<p>보조 management center 웹 인터페이스에서 Integration(통합) > Other Integrations(기타 통합) > High Availability(고가용성)를 클릭합니다. 보류 중인 디바이스 등록 테이블에서 보류 중인 디바이스의 IP 주소를 클릭한 다음 IP 주소를 threat defense의 퍼블릭 IP 주소로 변경합니다.</p> <p>또는</p> <ol style="list-style-type: none"> 1. threat defense 셸(shell)에 액세스하고 show managers 명령을 사용하여 스탠바이 management center 항목 식별자 값을 가져옵니다. 2. threat defense 셸(shell)에서 스탠바이 management center 호스트 이름을 퍼블릭 IP 주소로 편집합니다. 항목 식별자 값과 호스트 IP 주소를 사용하여 configure manager edit <standby_uuid> hostname <standby_ip> 명령을 실행합니다. <p>자세한 내용은 Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인, 15 페이지를 참고하십시오.</p>
고가용성 management center 간에 디바이스 구성 동기화 작업이 중지되었음	이제 디바이스 설정 기록 파일은 management center HA 동기화 중에 다른 설정 데이터와 병렬로 동기화됩니다. management center에서는 구성 기록 파일 동기화 작업을 모니터링하고 지난 6 시간 동안 동기화가 발생하지 않았으면 알람을 전송합니다. 이 상태 알람은 활성 및 대기 management center에 모두 표시됩니다.	활성 및 대기 management center 모두 성능 저하 상태에 진입합니다. Cisco 지원 팀에 문의하여 문제를 해결하십시오.

Firepower Management Center 고가용성을 위한 요구 사항

모델 지원

[하드웨어 요구 사항, 9 페이지](#)의 내용을 참조하십시오.

가상 모델 지원

가상 플랫폼 요건, 9 페이지의 내용을 참조하십시오.

지원되는 도메인

글로벌

사용자 역할

관리자

하드웨어 요구 사항

- 모든 management center 하드웨어는 고가용성을 지원합니다. 피어는 동일한 모델이어야 합니다.
- 피어는 서로 다른 데이터 센터에서 물리적 및 지리적으로 분리되어 있을 수 있습니다.
- 고가용성 구성에 대한 대역폭 요구 사항은 네트워크 크기, 매니지드 디바이스 수, 이벤트와 로그 양, 구성 업데이트 크기 및 빈도 등의 다양한 요인에 따라 달라집니다.
일반적인 management center 고가용성 구축은 100ms에 가까운 긴 레이턴시 네트워크의 경우 피어 간 최소 5MBps의 네트워크 대역폭이 권장됩니다.
- 기본 피어의 백업을 보조 피어로 복원하지 마십시오.
- [Management Center 고가용성 설정에 대한 라이선스 요구 사항, 10 페이지](#)도 참조하십시오.

가상 플랫폼 요건

두 개의 management center virtual 어플라이언스를 사용하여 고가용성(HA)을 설정하기 위한 요구 사항:

- VMware, AWS, OCI, Azure, KVM, Hyper-V, HyperFlex에 대해서만 management center virtual에서 지원됩니다.
- management center virtual 10, 25 및 300에서 지원됩니다.



참고 Management Center Virtual 300은 Hyper-V, Azure, HyperFlex에서 지원되지 않습니다.

- 고가용성 쌍의 디바이스 관리 용량은 동일해야 합니다. 예를 들어, management center virtual 25를 management center virtual 300과 페어링할 수 없습니다.
- threat defense 디바이스를 관리하려면 management center virtual 라이선스가 동일한 인스턴스 2개와 각 매니지드 디바이스에 대한 threat defense 엔타이틀먼트가 필요합니다. 버전 7.0 이하 클래식 디바이스만 관리하는 경우에는 management center virtual 엔타이틀먼트가 필요하지 않습니다.

자세한 내용은 [Management Center 고가용성 설정에 대한 라이선스 요구 사항, 10 페이지](#)를 참고하십시오.

소프트웨어 요구 사항

소프트웨어 버전, 침입 규칙 업데이트 버전, 취약성 데이터베이스 업데이트를 확인하려면 어플라이언스 정보 위젯에 액세스합니다. 이 위젯은 기본적으로 **Detailed Dashboard**(상세 대시보드) 및 **Summary Dashboard**(요약 대시보드)의 **Status**(상태) 탭에 나타납니다. 자세한 내용은 [어플라이언스 정보 위젯](#)을 참조해 주십시오.

- 고가용성 구성의 두 management center는 주(첫 번째 번호), 부(두 번째 번호), 유지 보수(세 번째 번호) 소프트웨어 버전이 동일해야 합니다.
- 고가용성 구성의 두 management center에는 동일한 침입 규칙 업데이트가 설치되어 있어야 합니다.
- 고가용성 구성의 두 management center에는 동일한 취약성 데이터베이스 업데이트가 설치되어 있어야 합니다.
- 고가용성 구성의 두 management center에는 동일한 버전의 LSP(Lightweight Security Package)가 설치되어 있어야 합니다.



경고! 두 management center의 소프트웨어 버전, 침입 규칙 업데이트 버전, 취약성 데이터베이스 업데이트 버전이 동일하지 않은 경우 고가용성을 설정할 수 없습니다.

Management Center 고가용성 설정에 대한 라이선스 요구 사항

각 디바이스에는 단일 management center 또는 고가용성 쌍(하드웨어 또는 가상)의 management center로 관리되는 동일한 라이선스가 필요합니다.

예: management center 쌍으로 관리되는 두 디바이스에 대해 고급 악성코드 보호를 활성화하고 싶은 경우, 2개의 악성코드 방어 라이선스와 TM 서브스크립션을 구매하고 액티브 management center을 Smart Software Manager에 등록한 뒤 두 기기의 라이선스를 액티브 management center에 할당합니다.

액티브 management center만 Smart Software Manager에 등록됩니다. 페일오버가 발생하면 시스템은 Smart Software Manager와 통신하여 원래 활성 management center에서 라이선스 등록을 해제하고 새로운 액티브 management center에 할당합니다.

특정 라이선스 예약 구축에서는 기본 management center에서만 특정 라이선스 예약이 요구됩니다.

하드웨어 Management Center

고가용성 쌍의 하드웨어 management center에 필요한 특별한 라이선스는 없습니다.

Management Center Virtual

라이선스가 동일한 두 개의 management center virtual가 필요합니다.

예: 10개의 디바이스를 관리하는 management center virtual 고가용성 쌍의 경우 다음을 사용할 수 있습니다.

- management center virtual 10 엔타이틀먼트 2개
- 디바이스 라이선스 10개

고가용성 쌍을 분리하면 보조 management center virtual와 연결된 management center virtual 엔타이틀먼트가 해제됩니다. (이 예에서는 독립형 management center virtual 10이 2개 있습니다.)

Management Center 고가용성의 전제조건

management center 고가용성 쌍을 설정하기 전에:

- 해당 보조 management center에서 해당 기본 management center에서 필요한 정책 내보내기 자세한 내용은 [컨피그레이션 내보내기](#)를 참고하십시오.
- 해당 보조 management center에 추가 장치가 부착되어 있지 않은지 확인하십시오. 해당 보조 management center에서 디바이스를 삭제하고 해당 기본 management center에 디바이스를 등록합니다. 자세한 내용은 [Cisco Secure Firewall Management Center 디바이스 구성 가이드](#)의 *Management Center*에서 디바이스 삭제 및 *Management Center*에 디바이스 추가를 참조하십시오.
- 해당 기본 management center에 정책을 가져옵니다. 자세한 내용은 [컨피그레이션 가져오기](#)를 참고하십시오.
- 해당 기본 management center에서 가져온 정책을 확인하고, 필요한 경우 편집하고, 적절한 장치에 구축합니다. 자세한 내용은 [Cisco Secure Firewall Management Center 디바이스 구성 가이드](#)의 구성 변경 사항 구축을 참조하십시오.
- 해당 기본 management center에 새로 추가된 디바이스에 적절한 라이선스를 연결합니다. 자세한 내용은 [단일 디바이스에 라이선스 할당](#)를 참조하십시오.

이제 고가용성 설정을 위한 진행이 가능합니다. 자세한 내용은 [Management Center 고가용성 설정, 11 페이지](#)를 참고하십시오.

Management Center 고가용성 설정

고가용성 설정에는 피어 간 대역폭 및 정책 수에 따라 최대 몇 시간까지 상당한 시간이 걸릴 수 있습니다. 또한 스탠바이 management center에 동기화되어야 하는 액티브 management center에 등록된 디바이스 수에 따라 다릅니다. 고가용성 피어의 상태를 확인하기 위해 고가용성 페이지를 볼 수 있습니다.

시작하기 전에

- 모든 management center이 고가용성 시스템 요구 사항을 준수하는지 확인하십시오. 자세한 내용은 [Firepower Management Center 고가용성을 위한 요구 사항, 8 페이지](#)를 참조하십시오.
- 고가용성을 설정하기 위한 사전 요건을 완료하였는지 확인합니다. 자세한 내용은 [Management Center 고가용성의 전제조건, 11 페이지](#)를 참고하십시오.

프로시저

-
- 단계 1 보조로 지정하려는 management center에 로그인합니다.
- 단계 2 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.
- 단계 3 고가용성을 선택합니다.
- 단계 4 이 management center의 역할에서 보조를 선택합니다.
- 단계 5 기본 **Firepower Management Center** 호스트 텍스트 상자에서 기본 management center의 호스트 이름 또는 IP 주소를 입력합니다.
- 기본 management center에 피어 management center(공용 또는 프라이빗 IP 주소일 수 있음)에서 연결할 수 있는 IP 주소가 없는 경우에는 비워 둘 수 있습니다. 이 경우 등록 키와 고유 **NAT ID** 필드를 모두 사용하십시오. HA 연결을 활성화하려면 하나 이상의 management center에 대한 IP 주소를 지정해야 합니다.
- 단계 6 등록 키 텍스트 상자에서 일회용 등록 키를 입력합니다.
- 등록 키는 최대 37자의 사용자가 정의한 영숫자 값입니다. 이 등록 키는 보조 및 기본 management center을 등록할 때 사용합니다.
- 단계 7 기본 IP 주소를 지정하지 않거나 기본 management center에서 보조 IP 주소를 지정하지 않을 경우 고유 **NAT ID** 필드에서 고유의 영숫자 ID를 입력합니다. 자세한 내용은 [NAT 환경](#)를 참조하십시오.
- 단계 8 **Register(등록)**를 클릭합니다.
- 단계 9 Admin 액세스 권한이 있는 계정을 사용하여 기본으로 지정할 management center에 로그인합니다.
- 단계 10 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.
- 단계 11 고가용성을 선택합니다.
- 단계 12 이 management center의 역할에서 기본을 선택합니다.
- 단계 13 보조 **Firepower Management Center** 호스트 텍스트 상자에서 보조 management center의 호스트 이름 또는 IP 주소를 입력합니다.
- 보조 management center에 피어 management center(공용 또는 프라이빗 IP 주소일 수 있음)에서 연결 가능한 IP 주소가 없는 경우에는 비워 둘 수 있습니다. 이 경우 등록 키와 고유 **NAT ID** 필드를 모두 사용하십시오. HA 연결을 활성화하려면 하나 이상의 management center에 대한 IP 주소를 지정해야 합니다.
- 단계 14 6단계에서 사용한 것과 동일한 1회용 등록 키를 등록 키 텍스트 상자에 입력합니다.
- 단계 15 필요한 경우 고유 **NAT ID** 텍스트 상자에 7단계에서 사용한 것과 동일한 NAT ID를 입력합니다.

단계 16 **Register**(등록)를 클릭합니다.

다음에 수행할 작업

management center 고가용성 쌍을 설정한 후 액티브 management center에 등록된 디바이스는 자동으로 스탠바이 management center에 등록됩니다.



참고 등록된 디바이스에 NAT IP 주소가 있는 경우 자동 디바이스 등록이 실패하고 보조 management center의 High Availability(고가용성) 페이지가 디바이스를 로컬, 보류 중으로 표시합니다. 스탠바이 management center 고가용성 페이지에 표시된 디바이스에 다른 NAT IP 주소를 할당할 수 있습니다. 자동 등록이 스탠바이 management center에 실패하지만 디바이스가 액티브 Firepower Management Center에 등록된 것으로 표시되는 경우 [Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인, 15 페이지](#)를 참조합니다.

Management Center 고가용성 상태 보기

액티브 및 스탠바이 management center를 확인한 후 로컬 management center와 해당 피어에 대한 정보를 볼 수 있습니다.



참고 이때 로컬 피어는 시스템 상태를 확인하는 어플라이언스를 가리킵니다. 원격 피어는 액티브 또는 스탠바이 상태에 관계없이 다른 어플라이언스를 가리킵니다.

프로시저

단계 1 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 2 **Integration**(통합) > **Other Integrations**(기타 통합)을 선택합니다.

단계 3 고가용성을 선택합니다.

다음은 볼 수 있습니다.

요약 정보

- 고가용성 쌍의 상태 스탠바이 유닛이 액티브 유닛에서 구성 변경 사항을 수신하면 올바르게 작동하는 시스템의 상태가 "정상"과 "동기화 작업이 진행 중입니다."로 표시됩니다.
- 고가용성 쌍의 현재 동기화 상태
- 액티브 피어의 IP 주소와 최근 동기화 시간
- 스탠바이 피어의 IP 주소와 최근 동기화 시간

시스템 상태

- 두 피어의 IP 주소
- 두 피어의 운영 체제
- 두 피어의 소프트웨어 버전
- 두 피어의 어플라이언스 모델

참고 활성 management center에서만 내보내기 제어 및 컴플라이언스 상태를 볼 수 있습니다.

Management Center 고가용성 쌍에서 동기화된 구성

두 management center 사이에 고가용성을 설정하면 다음 설정 데이터가 동기화됩니다.

- 라이선스 등록
- 액세스 제어 정책
- 침입 규칙
- 악성코드 및 파일 정책
- DNS 정책
- ID 정책
- SSL 정책
- 사전 필터 정책
- 네트워크 검색 규칙
- 애플리케이션 탐지기
- 상관 관계 정책 규칙
- 알림
- 스캐너
- 응답 그룹
- 조사 이벤트에 대한 외부 리소스의 상황별 교차 실행
- 보안정책 교정 설정을 위해 두 management center에 사용자 정의 모듈을 설치해야 합니다. 보안 정책 교정 설정에 대한 자세한 내용은 [교정 모듈 관리](#)를 참조하십시오.

고가용성 쌍의 Management Center 데이터베이스에 대한 외부 액세스 구성

고가용성 설정에서는 활성 피어만 사용하여 데이터베이스에 대한 외부 액세스를 구성하는 것이 좋습니다. 외부 데이터베이스 액세스를 위해 대기 피어를 구성하는 경우 연결이 자주 끊어집니다. 연결을 복원하려면 스탠바이 피어의 동기화를 **쌍을 이룬 Management Center 간에 통신 일시 중지**하고 **쌍을 이룬 Management Center 간에 통신 다시 시작**해야 합니다. management center에 대한 외부 데이터베이스 액세스를 활성화하는 방법에 대한 내용은 **데이터베이스에 대한 외부 액세스 활성화**를 참조하십시오.

Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인

스탠바이 management center에 자동 디바이스 등록이 실패하지만 액티브 management center로 등록된 경우 다음 단계를 완료합니다.



경고! 보조 management center RMA를 수행하거나 보조 management center를 추가하는 경우 매니지드 디바이스가 등록 취소되며, 결과적으로 구성이 삭제될 수 있습니다.

프로시저

단계 1 액티브 management center에서 디바이스를 삭제합니다. [Cisco Secure Firewall Management Center 디바이스 구성 가이드](#)에서 *management center*의 디바이스 삭제(등록 취소)를 참조하십시오.

단계 2 스탠바이 management center에서 디바이스의 자동 등록을 트리거하려면 다음 단계를 완료합니다.

1. 영향을 받는 디바이스의 CLI에 로그인합니다.
2. CLI 명령을 실행합니다. **configure manager delete**.
이 명령은 현재 management center을 비활성화하고 제거합니다.
3. CLI 명령을 실행합니다. **configure manager add**.
이 명령은 management center에 연결하기 위한 디바이스를 구성합니다.

팁 액티브 management center에 한해 디바이스의 원격 관리를 구성합니다. 고가용성을 설정하면 디바이스가 자동으로 스탠바이 management center에 등록됩니다.

4. 액티브 management center에 로그인하고 디바이스를 등록합니다.

단계 3 스탠바이 management center가 NAT 뒤에 있는 경우 다음 단계를 완료하여 스탠바이 management center의 호스트 이름을 편집합니다.

1. threat defense 셸(shell)에 액세스하고 `show managers` 명령을 사용하여 스탠바이 management center 항목 식별자 값을 가져옵니다.
2. threat defense 셸(shell)에서 스탠바이 management center 호스트 이름을 퍼블릭 IP 주소로 편집합니다. 항목 식별자 값과 호스트 IP 주소를 사용하여 `configure manager edit <standby_uuid> hostname <standby_ip>` 명령을 실행합니다.

Management Center 고가용성 쌍에서 피어 전환

시스템이 일부 기능을 액티브 management center로 제한하므로 해당 어플라이언스가 실패하면 스탠바이 management center를 액티브로 승격해야 합니다.

프로시저

단계 1 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 2 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.

단계 3 고가용성을 선택합니다.

단계 4 액티브를 스탠바이로, 스탠바이를 액티브로 로컬 역할을 변경하려면 피어 역할 전환을 선택합니다. 그러면 기본 또는 보조 지정은 변경되지 않은 채 두 피어 간 역할이 전환됩니다.

쌍을 이룬 Management Center 간에 통신 일시 중지

일시적으로 고가용성을 비활성화하려는 경우 management center 간의 통신 채널을 비활성화할 수 있습니다. 액티브 피어에서 동기화를 중단하면 액티브 또는 스탠바이 피어 중 하나에서 동기화를 재개할 수 있습니다. 그러나 스탠바이 피어의 동기화를 중단하면 스탠바이 피어에서만 동기화를 재개할 수 있습니다.

프로시저

단계 1 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 2 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.

단계 3 고가용성을 선택합니다.

단계 4 동기화 일시 정지를 선택합니다.

쌍을 이룬 Management Center 간에 통신 다시 시작

일시적으로 고가용성을 비활성화하려는 경우 management center 간 통신 채널을 활성화하여 고가용성을 재시작할 수 있습니다. 액티브 유닛에서 동기화를 중단한 경우 스탠바이 또는 액티브 유닛 모두에서 동기화를 재개할 수 있습니다. 그러나 스탠바이 유닛의 동기화를 중단하면 스탠바이 유닛에서만 동기화를 재개할 수 있습니다.

프로시저

-
- 단계 1 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.
 - 단계 2 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.
 - 단계 3 고가용성을 선택합니다.
 - 단계 4 동기화 재개를 선택합니다.
-

고가용성 쌍의 Management Center IP 주소 변경

고가용성 피어 중 하나에 대한 IP 주소가 변경되면 고가용성이 저하 상태에 진입합니다. 고가용성을 복구하려면 수동으로 IP 주소를 변경해야 합니다.

프로시저

-
- 단계 1 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.
 - 단계 2 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.
 - 단계 3 고가용성을 선택합니다.
 - 단계 4 피어 관리자를 선택합니다.
 - 단계 5 **Edit(수정)** (✎)를 선택합니다.
 - 단계 6 시스템의 컨텍스트 내에서만 사용되는 어플라이언스의 표시 이름을 입력합니다.
다른 표시 이름을 입력해도 어플라이언스에 대한 호스트 이름은 변경되지 않습니다.
 - 단계 7 FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 유효한 IP 주소(호스트 이름) 또는 호스트 IP 주소를 입력합니다.
 - 단계 8 **Save(저장)**를 클릭합니다.
-

Management Center 고가용성 비활성화

프로시저

단계 1 고가용성 쌍의 management center 중 하나에 로그인합니다.

단계 2 **Integration(통합) > Other Integrations(기타 통합)**을 선택합니다.

단계 3 고가용성을 선택합니다.

단계 4 고가용성 분리를 선택합니다.

단계 5 관리되는 디바이스를 처리하기 위해 다음 옵션 중 하나를 선택합니다.

- 이 management center의 모든 관리되는 디바이스를 제어하기 위해 이 콘솔에서 등록된 디바이스 관리를 선택합니다. 피어에서 모든 디바이스가 등록 해제됩니다.
- 다른 management center의 모든 관리되는 디바이스를 제어하기 위해 피어 콘솔에서 등록된 디바이스 관리를 선택합니다. 이 management center에서 모든 디바이스가 등록 해제됩니다.
- 모든 디바이스 관리를 중지하려면 두 콘솔에서 등록된 디바이스 관리 중지를 선택합니다. 두 management center에서 모든 디바이스가 등록 해제됩니다.

참고 보조 management center에서 등록된 디바이스를 관리하도록 선택할 경우 디바이스는 기본 management center에서 등록 해제됩니다. 디바이스가 이제 보조 management center에서 관리되도록 등록됩니다. 그러나 이런 디바이스에 적용된 라이선스는 고가용성 해제 작업에 의해 등록 해제됩니다. 이제 보조 management center에서 디바이스 라이선스 재등록(활성화)를 진행해야 합니다. 자세한 내용은 [매니저드 디바이스에 라이선스 할당](#)를 참조하십시오.

단계 6 **OK(확인)**를 클릭합니다.

고가용성 쌍의 Management Center 교체

management center 고가용성 쌍에서 장애가 발생한 장치를 교체하는 경우 다음 절차 중 하나를 따라야 합니다. 다음 표는 4개의 오류 상황과 해당 교체 절차를 설명합니다.

오류 상태	데이터 백업 상태	교체 절차
기본 management center 오류	데이터 백업 성공	오류가 발생한 기본 Management Center 교체(백업 성공), 19 페이지
	데이터 백업 실패	오류가 발생한 기본 Management Center 교체(백업 실패), 20 페이지

오류 상태	데이터 백업 상태	교체 절차
보조 management center 오류	데이터 백업 성공	오류가 발생한 보조 Management Center 교체(백업 성공), 21 페이지
	데이터 백업 실패	오류가 발생한 보조 Management Center 교체(백업 실패), 22 페이지

오류가 발생한 기본 **Management Center** 교체(백업 성공)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 기본 management center인 *FMC1*을 교체하는 단계를 설명합니다.

시작하기 전에

오류가 발생한 기본 management center의 데이터 백업이 성공했는지 확인합니다.

프로시저

단계 1 오류가 발생한 management center - *FMC1*에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 2 기본 management center - *FMC1*에 오류가 발생하면 보조 management center인 *FMC2*의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 자세한 내용은 [Management Center 고가용성 쌍에서 피어 전환, 16 페이지](#)를 참고하십시오.

이때 보조 management center - *FMC2*를 액티브로 전환합니다.

기본 management center - *FMC1*이 교체될 때까지 *FMC2*를 액티브 management center로 사용할 수 있습니다.

주의 management center 고가용성을 *FMC2*에서 분리하지 마십시오. (오류 발생 전에) *FMC1*에서 *FMC2*에 동기화된 라이선스가 *FMC2*에서 제거되어 *FMC2*에서 구축 작업을 수행할 수 없게 됩니다.

단계 3 *FMC1*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.

단계 4 *FMC1*에서 생성한 데이터 백업을 새 management center에 복원합니다.

단계 5 *FMC2*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

새 management center 및 *FMC2* 모두 액티브 피어이므로 고가용성에 스플릿 브레인이 발생합니다.

단계 6 management center 웹 인터페이스가 액티브 어플라이언스를 선택하도록 할 경우 *FMC2*를 액티브로 선택합니다.

이때 *FMC2*의 최신 설정이 새 management center - *FMC1*에 동기화됩니다.

단계 7 설정 동기화가 성공하면 보조 management center - *FMC2*의 웹 인터페이스에 액세스하여 기본 management center - *FMC1*의 역할을 액티브로 전환합니다. 자세한 내용은 [Management Center 고가용성 쌍에서 피어 전환, 16 페이지](#)를 참고하십시오.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

오류가 발생한 기본 Management Center 교체(백업 실패)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 실패한 경우 오류가 발생한 기본 management center인 *FMC1*을 교체하는 단계를 설명합니다.

프로시저

단계 1 오류가 발생한 management center - *FMC1*에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 2 기본 management center - *FMC1*에 오류가 발생하면 보조 management center인 *FMC2*의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 자세한 내용은 [Management Center 고가용성 쌍에서 피어 전환, 16 페이지](#)를 참고하십시오.

이때 보조 management center - *FMC2*를 액티브로 전환합니다.

기본 management center - *FMC1*이 교체될 때까지 *FMC2*를 액티브 management center로 사용할 수 있습니다.

주의 management center 고가용성을 *FMC2*에서 분리하지 마십시오. (오류 발생 전에) *FMC1*에서 *FMC2*에 동기화된 라이선스가 *FMC2*에서 제거되어 *FMC2*에서 구축 작업을 수행할 수 없게 됩니다.

단계 3 *FMC1*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.

단계 4 *FMC2*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 5 management center - *FMC2* 중 하나를 Cisco Smart Software Manager에서 등록 취소합니다. 자세한 내용은 [등록 취소Management Center](#)을 참고하십시오.

management center을 Cisco Smart Software Manager에서 등록 취소하면 가상 어카운트에서 Management Center가 제거됩니다. management center와 연결되는 모든 라이선스 엔타이틀먼트를 가상 어카운트에 다시 릴리스합니다. 등록 취소 후 라이선스 기능에 대한 어떤 업데이트 또는 변경도 허용되지 않는 부분에서 management center가 Enforcement(시행) 모드를 입력합니다.

단계 6 보조 management center - *FMC2*의 웹 인터페이스에 액세스하여 management center 고가용성을 해제합니다. 자세한 내용은 [Management Center 고가용성 비활성화, 18 페이지](#)를 참고하십시오. 관리되는 디바이스를 처리하기 위한 옵션 선택 메시지가 표시되면 이 콘솔에서 등록된 디바이스 관리를 선택합니다.

따라서 보조 management center - *FMC2*에서 동기화된 라이선스가 제거되고 *FMC2*에서 구축 작업을 수행할 수 없습니다.

- 단계 7 management center - *FMC2*를 기본으로 설정하고 management center - *FMC1*을 보조로 설정하여 management center 고가용성을 다시 설정합니다. 자세한 내용은 [Management Center 고가용성 설정, 11 페이지](#)를 참조하십시오.
- 단계 8 기본 management center - *FMC2*에 스마트 라이선스를 등록합니다. 자세한 내용은 [Management Center 를 Smart Software Manager로 등록](#)를 참조하십시오.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

오류가 발생한 보조 Management Center 교체(백업 성공)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 보조 management center인 *FMC2*를 교체하는 단계를 설명합니다.

시작하기 전에

오류가 발생한 보조 management center의 데이터 백업이 성공했는지 확인합니다.

프로시저

- 단계 1 오류가 발생한 management center - *FMC2*에 대한 교체를 요청하려면 지원팀에 문의합니다.
- 단계 2 기본 management center - *FMC1*을 액티브 management center로 계속 사용합니다.
- 단계 3 *FMC2*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.
- 단계 4 *FMC2*에서 생성한 데이터 백업을 새 management center에 복원합니다.
- 단계 5 *FMC1*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.
- 단계 6 (중단된 경우) 기본 management center - *FMC1*의 최신 설정을 동기화하기 위해 새 management center의 웹 인터페이스 *FMC2*에서 데이터 동기화를 재개합니다. 자세한 내용은 [쌍을 이룬 Management Center 간에 통신 다시 시작, 17 페이지](#)를 참고하십시오.
- 클래식 및 스마트 라이선스가 원활하게 작동합니다.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

오류가 발생한 보조 Management Center 교체(백업 실패)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 보조 management center인 *FMC2*를 교체하는 단계를 설명합니다.

프로시저

-
- 단계 1 오류가 발생한 management center - *FMC2*에 대한 교체를 요청하려면 지원팀에 문의합니다.
 - 단계 2 기본 management center - *FMC1*을 액티브 management center로 계속 사용합니다.
 - 단계 3 *FMC2*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.
 - 단계 4 *FMC1*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.
 - 단계 5 기본 management center - *FMC1*의 웹 인터페이스에 액세스하여 management center 고가용성을 해제합니다. 자세한 내용은 [Management Center 고가용성 비활성화, 18 페이지](#)를 참고하십시오. 관리되는 디바이스를 처리하기 위한 옵션 선택 메시지가 표시되면 이 콘솔에서 등록된 디바이스 관리를 선택합니다.
 - 단계 6 management center - *FMC2*를 기본으로 설정하고 management center - *FMC1*을 보조로 설정하여 management center 고가용성을 다시 설정합니다. 자세한 내용은 [Management Center 고가용성 설정, 11 페이지](#)를 참조하십시오.
 - 고가용성이 성공적으로 설정된 경우 기본 management center - *FMC1*의 최신 설정이 보조 management center - *FMC2*에 동기화됩니다.
 - 클래식 및 스마트 라이선스가 원활하게 작동합니다.
-

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

Management Center 고가용성 재해 복구

재해 복구 상황에서는 수동 전환을 수행해야 합니다. 기본 management center - *FMC1*에 오류가 발생하면 보조 management center인 *FMC2*의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 이는 보조(*FMC2*)에 장애가 발생하는 경우에도 반대로 적용됩니다. 자세한 내용은 [Management Center 고가용성 쌍에서 피어 전환, 16 페이지](#)를 참고하십시오.

실패한 management center 복원에 대해서는 [고가용성 쌍의 Management Center 교체, 18 페이지](#)의 내용을 참조하십시오.

고가용성 쌍의 Management Center 복원(하드웨어 장애 없음)

하드웨어 장애가 없는 경우 management center 고가용성 쌍을 복원하려면 다음 절차를 수행합니다.

- 기본 Management Center에서 백업 복원, 23 페이지
- 보조 Management Center에서 백업 복원, 23 페이지

기본 Management Center에서 백업 복원

시작하기 전에

- 관리 센터의 하드웨어 오류 및 교체가 없습니다.
- 백업 및 복원 프로세스를 잘 알고 있어야 합니다. [백업/복구](#)를 참조하십시오.

프로시저

-
- 단계 1 기본 management center의 백업을 사용할 수 있는지 확인합니다(/var/sf/backup/의 로컬 스토리지 또는 원격 네트워크 볼륨).
 - 단계 2 기본 management center에서 동기화를 일시 정지합니다. **Integration(통합)** > **Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 일시 정지합니다.
 - 단계 3 기본 management center에서 백업을 복원합니다. 복원이 완료되면 management center가 재부팅됩니다.
 - 단계 4 기본 management center가 활성 상태이고 해당 사용자 인터페이스에 연결할 수 있으면 보조 management center에서 동기화를 다시 시작합니다. **Integration(통합)** > **Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 다시 시작합니다.
-

보조 Management Center에서 백업 복원

시작하기 전에

- 관리 센터의 하드웨어 오류 및 교체가 없습니다.
- 백업 및 복원 프로세스를 잘 알고 있어야 합니다. [백업/복구](#)를 참조하십시오.

프로시저

-
- 단계 1 보조 management center의 백업을 사용할 수 있는지 확인합니다(/var/sf/backup/의 로컬 스토리지 또는 원격 네트워크 볼륨).
 - 단계 2 기본 management center에서 동기화를 일시 정지합니다. **Integration(통합) > Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 일시 정지합니다.
 - 단계 3 보조 management center에서 백업을 복원합니다. 복원이 완료되면 management center가 재부팅됩니다.
 - 단계 4 보조 management center가 활성화 상태이고 해당 사용자 인터페이스에 연결할 수 있으면 기본 management center에서 동기화를 다시 시작합니다. **Integration(통합) > Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 다시 시작합니다.
-

고가용성에 Management Center 통합 백업

활성 management center에서 통합 백업을 수행할 수 있으며, 이 경우 활성화 및 대기 management center 모두에 대해 단일 백업 파일이 생성됩니다. 통합 백업은 설정 전용 백업에만 적용됩니다. 이벤트 또는 TID 백업이 필요한 경우 활성화 및 대기 management center에 대해 별도의 백업을 수행해야 합니다. 설정 전용 백업을 선택하면 기본적으로 통합 백업이 적용됩니다. 통합 백업에서 활성화 management center이 대기 management center에서 백업 tar 파일을 가져올 수 없는 경우, 복원에 사용할 수 있는 활성 유닛에 대한 일반 백업 파일이 생성됩니다. 통합 백업은 일반 백업에 비해 다음과 같은 몇 가지 이점이 있습니다.

- 통합 백업을 사용하는 경우 활성화 및 대기 management center에 대해 별도로 백업을 수행할 필요가 없습니다.
- 백업 및 스토리지 제약 조건의 중복 데이터는 통합 백업에서 제거됩니다.
- 일반 백업에서 기본 유닛에 오류가 발생하고 보조 유닛 백업을 사용할 수 없는 경우에는 보조 RMA에 대한 고가용성 쌍을 해제해야 했습니다. 이러한 상황은 통합 백업에서 해결됩니다.
- 일반적으로 대기 유닛의 백업은 예약할 수 없습니다. 예약된 통합 백업에서는 활성화 및 대기 유닛의 백업이 수행됩니다.
- 통합 백업을 실행하는 동안 대기 유닛에서 백업을 수행하기 위해 HA 동기화를 일시 중지할 필요가 없습니다.

예기치 않은 사고가 발생하는 경우 통합 백업을 사용하여 새 RMA 디바이스를 복구할 수 있습니다. 통합 백업 파일은 이름으로 식별할 수 있습니다. 통합 백업 파일 이름에 접두사 "Unified"가 추가됩니다. 복원할 management center을 선택하고 해당 상태(활성/대기)를 선택할 수도 있습니다.

스플릿 브레인 충돌을 방지하기 위해 복원된 management center의 적절한 상태를 선택해야 합니다.

통합 백업에서 Management Center 복구

통합 백업에서 management center를 복원하려면 이 절차를 사용합니다(구성 전용).

프로시저

단계 1 복구하려는 management center에 로그인합니다.

단계 2 시스템 (⚙) > **Tools(툴)** > **Backup/Restore(백업/복구)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 통합 백업 파일을 포함하여 로컬 및 원격으로 저장된 모든 백업 파일이 나열됩니다(구성 전용).

통합 백업 파일이 목록에 없고 로컬 컴퓨터에 저장한 경우 **Upload Backup(백업 업로드)**을 클릭합니다. **백업 및 원격 스토리지 관리**의 내용을 참조하십시오.

단계 3 복원하려는 통합 백업 파일을 선택하고 **Restore(복원)**를 클릭합니다.

단계 4 **Restore Backup(백업 복원)** 페이지에서 복원할 유닛을 선택합니다. 통합 백업은 기본 및 보조 management center의 백업 구성을 저장하므로 복구할 유닛을 선택해야 합니다.

단계 5 복원된 management center의 상태를 선택하려면 **Active(활성)** 또는 **Standby(대기)** 라디오 버튼을 클릭합니다. 두 피어가 모두 동일한 역할 및 상태 설정을 사용하지 않도록 작동 중인 관리 센터의 역할 및 상태를 반드시 확인해야 합니다. 복원 시 관리 센터에 대해 잘못된 역할 및 상태를 선택하면 HA 실패가 발생할 수 있습니다.

단계 6 **Restore(복원)**를 클릭한 다음 **Confirm Restore(복원 확인)**를 클릭하여 복원을 시작합니다.

Management Center 고가용성 히스토리

기능	최소 Management Center	최소 Threat Defense	세부 사항
고가용성 Management Center를 위한 단일 백업 파일.	7.4.1	Any(모든)	고가용성 쌍으로 구성된 활성 Management Center의 구성 전용 백업을 수행할 경우, 이제 시스템에서는 단일 백업 파일을 생성하며 해당 파일을 사용하여 각 유닛을 복원할 수 있습니다.
management center HA 동기화 실패를 줄이고 동기화 시간을 개선했습니다.	7.4.1	7.4.1	레이턴시가 긴 네트워크에서 더 큰 구성 기록 파일로 인한 HA 동기화 실패를 방지하기 위해 이제 management center HA 동기화 중에 디바이스 구성 기록 파일이 다른 구성 데이터와 병렬로 동기화됩니다. 이 향상된 기능은 HA 동기화 실패를 줄이고 management center HA 동기화 시간을 개선합니다. management center에서는 구성 기록 파일 동기화 작업을 모니터링하고 HA 동기화 시간이 초과되면 알려줍니다.

기능	최소 Management Center	최소 Threat Defense	세부 사항
Hyper-V에서 고가용성을 지원합니다.	7.4.0	7.4.0	이제 Hyper-V에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 9 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항 , 10 페이지를 참조하십시오.
Azure 및 KVM에서 고가용성을 지원합니다.	7.3.0	7.3.0	이제 Azure 및 KVM에 대해 management center virtual에서 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 9 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항 , 10 페이지를 참조하십시오.
AWS 및 OCI에서 고가용성을 지원합니다.	7.1.0	7.1.0	이제 AWS 및 OCI에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 9 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항 , 10 페이지를 참조하십시오.
HyperFlex의 고가용성을 지원합니다.	7.0.0	7.0.0	이제 HyperFlex에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 9 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항 , 10 페이지를 참조하십시오.
VMware의 고가용성을 지원합니다.	6.7.0	6.7.0	이제 VMware에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 9 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항 , 10 페이지를 참조하십시오.
SSO(Single Sign-On)	6.7.0	6.7.0	SSO(Single Sign-On)를 위해 고가용성 쌍의 멤버 하나 또는 둘 다를 구성할 때는 특별한 고려 사항이 있습니다.

번역에 관하여

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