백업/복구

- 백업 및 복원 정보, 1 페이지
- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지
- Management Center 또는 매니지드 디바이스 백업, 10 페이지
- Management Center 및 매니지드 디바이스 복원, 15 페이지
- 백업 및 원격 스토리지 관리, 31 페이지
- 백업 및 복원 기록, 35 페이지

백업 및 복원 정보

재해부터 복구할 수 있는 능력은 모든 시스템 유지 보수 계획에서 필수적인 부분입니다. 재해 복구 계획의 일환으로, 정기적인 백업을 수행하여 원격 위치를 보호하는 것이 좋습니다.

온디맨드 백업

management center 및 여러 threat defense 디바이스에 대해 management center에서 온 디맨드 백업을 수행할 수 있습니다.

자세한 내용은 Management Center 또는 매니지드 디바이스 백업, 10 페이지를 참고하십시오.

예약 백업

management center에서 스케줄러를 사용하여 백업을 자동화할 수 있습니다. management center에서의 원격 디바이스 백업은 예약할 수 없습니다.

management center 설정 프로세스는 매주 설정 전용 백업을 예약하여 로컬에 저장합니다. 이는 전체 오프 사이트 백업을 대체하지 않습니다. 초기 설정이 완료되면 예약된 작업을 검토하고 조직의 요구에 맞게 조정해야 합니다.

자세한 내용은 예약 백업를 참고하십시오.

백업 파일 저장

로컬로 백업을 저장할 수 있습니다. 그러나 NFS, SMB 또는 SSHFS 네트워크 볼륨을 원격 스토리지로 마운트하여 management center 및 매니지드 디바이스를 안전한 원격 위치에 백업하는 것이 좋습니다. 이렇게 하면 모든 후속 백업이 해당 볼륨에 복사되지만, 계속해서 management center를 사용하여 백업을 관리할 수 있습니다.

자세한 내용은 원격 스토리지 디바이스 및 백업 및 원격 스토리지 관리, 31 페이지를 참조하십시오.

Management Center 및 매니지드 디바이스 복원

Backup Management(백업 관리) 페이지에서 management center를 복구합니다. SD 카드와 재설정 버튼을 사용하는 ISA 3000 제로 터치 복원을 제외하고 threat defense CLI를 사용하여 threat defense 디바이스를 복원해야 합니다..

자세한 내용은 Management Center 및 매니지드 디바이스 복원, 15 페이지를 참고하십시오.

백업이란**?**

Management Center 백업에는 다음이 포함될 수 있습니다.

- 설정

  management center 웹 인터페이스에서 설정할 수 있는 모든 설정은 원격 스토리지 및 감사 로그 서버 인증서 설정을 제외하고 설정 백업에 포함됩니다. 다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는 TID 데이터만 백업할 수는 없습니다.

- 이벤트.

  이벤트 백업에는 management center 데이터베이스의 모든 이벤트가 포함됩니다. 그러나 management center 이벤트 백업에는 침입 이벤트 검토 상태가 포함되지 않습니다. 복구된 침입 이벤트는 Reviewed Events(검토된 이벤트) 페이지에 나타나지 않습니다.

- TID(Threat Intelligence Director) 데이터.

  자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *threat intelligence director* 데이터 백업 및 복원 정보를 참조하십시오.

디바이스 백업은 항상 설정 전용입니다.

복구되는 항목

설정을 복구하면 극히 드문 예외를 제외하고 모든 백업된 설정을 덮어씁니다. management center에서 이벤트 및 TID 데이터를 복구하면 침입 이벤트를 제외한 모든 기존 이벤트 및 TID 데이터를 덮어씁니다.

다음 사항을 이해하고 계획해야 합니다.

- 백업되지 않은 항목은 복구할 수 없습니다.

  Management Center 설정 백업에는 원격 스토리지 및 감사 로그 서버 인증서 설정이 포함되지 않으므로 복구 후에 이러한 설정을 다시 구성해야 합니다. 또한 management center 이벤트 백업에

는 침입 이벤트 검토 상태가 포함되지 않으므로 복구된 침입 이벤트는 Reviewed Events(검토된 이벤트) 페이지에 나타나지 않습니다.

- VPN 인증서 복구에 실패했습니다.

  threat defense 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense 디바이스에서 VPN 인증서 및 모든 VPN 구성을 제거합니다. threat defense 디바이스를 복구한 후에는 모든 VPN 인증서를 다시 추가/다시 등록하고 디바이스를 다시 구축해야 합니다.

- 구성된 management center 복구 - 공장 설정으로 새로 고침 또는 이미지 재설치 대신 침입 이벤트와 파일 목록이 병합됩니다.

  management center 이벤트 복구 프로세스는 침입 이벤트를 덮어쓰지 않습니다. 대신 백업의 침입 이벤트가 데이터베이스에 추가됩니다. 중복을 방지하려면 복구 전에 기존 침입 이벤트를 삭제하십시오.

  management center 설정 복구 프로세스는 악성코드 대응 에서 사용되는 정상 및 사용자 지정 탐지 파일 목록을 덮어쓰지 않습니다. 대신 기존 파일 목록을 백업의 파일 목록과 병합합니다. 파일 목록을 교체하려면 복구하기 전에 기존 파일 목록을 삭제하십시오.

백업 및 복구 요구 사항

백업 및 복구에는 다음 요구 사항이 있습니다.

모델 요구 사항**:** 백업

다음을 백업할 수 있습니다.

- 이 management center
- threat defense 독립형 디바이스, 네이티브 인스턴스, 컨테이너 인스턴스, 고가용성 쌍 및 클러스터
- 프라이빗 클라우드 독립형 디바이스, 고가용성 쌍 및 클러스터용 threat defense virtual

백업은 다음에 대해 지원되지 않습니다.

- 퍼블릭 클라우드용 threat defense virtual

백업 및 복구가 지원되지 않는 디바이스를 교체해야 한다면 디바이스별 설정을 수동으로 다시 생성해야 합니다. 하지만 management center 백업은 매지니드 디바이스에 구축하는 정책과 다른 구성은 백업하지 않으며, 디바이스에서 이미 management center로 전송된 이벤트도 백업하지 않습니다.

모델 요구 사항**:** 복구

교체 매니지드 디바이스는 교체하려는 디바이스와 동일한 모델이어야 하며 동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스를 사용해야 합니다.

management center의 경우 RMA 시나리오에서 백업 및 복구를 사용할 수 있을 뿐 아니라 management center 간에 설정 및 이벤트를 마이그레이션할 수도 있습니다. 지원되는 대상 및 대상 모델을 포함한 자세한 내용은 Firepower Management Center 모델 마이그레이션 가이드의 내용을 참조하십시오.

버전 요구 사항

모든 백업의 첫 번째 단계로 패치 레벨을 참고합니다. 백업을 복구하려면 이전 어플라이언스와 새 어플라이언스에서 패치를 포함하여 동일한 소프트웨어 버전을 실행해야 합니다.

또한 Firepower 4100/9300 섀시에서 소프트웨어를 복구하려면 섀시에서 호환되는 FXOS 버전을 실행해야 합니다.

management center 백업의 경우 동일한 VDB 또는 SRU가 없어도됩니다. 그러나 백업을 복구하면 기존 VDB가 백업 파일의 VDB로 대체됩니다.

라이선스 요건

모범 사례 및 절차에 설명된 대로 라이선싱 또는 고아 엔타이틀먼트 문제를 해결합니다. 라이선싱 충돌이 발견되면 Cisco TAC에 문의하십시오.

도메인 요구 사항

작업:

- management center 백업 또는 복구: 전역 전용.
- management center에서 디바이스 백업: 전역 전용.
- 디바이스 복구 : 없음. CLI에서 로컬로 디바이스를 복구합니다.

다중 도메인 구축에서는 이벤트/TID 데이터만백업할 수는 없습니다. 구성도 함께 백업해야 합니다.

백업 및 복원 지침 및 제한 사항

백업 및 복원에는 다음과 같은 지침 및 제한 사항이 있습니다.

백업 및 복원은 재해 복구**/RMA**에 사용됩니다**.**

백업 및 복원은 주로 RMA 시나리오를 위한 것입니다. 결함이 있거나 고장난 물리적 어플라이언스의 복원 프로세스를 시작하기 전에, Cisco TAC에 연락해 교체 하드웨어를 요청하십시오.

백업 및 복원을 사용하여 management center 간에 구성 및 이벤트를 마이그레이션할 수도 있습니다. 따라서 조직의 성장, 물리적 구현에서 가상 구현으로의 마이그레이션, 하드웨어 새로 고침 등의 기술적 또는 비즈니스적 이유로 인해 management center를 쉽게 교체할 수 있습니다.

백업 및 복원은 구성 가져오기**/**내보내기가 아닙니다**.**

백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 또는 디바이스 간에 구성을 복사하거나, 새 구성을 테스트하는 동안 다른 구성을 저장하지는 마십시오. 대신 가져오기/내보내기 기능을 사용해야 합니다.

예를 들어 threat defense 디바이스 백업에는 디바이스의 관리 IP 주소 및 디바이스가 관리 management center에 연결하는 데 필요한 모든 정보가 포함됩니다. 다른 management center에서 매니지드 디바이스에 threat defense 백업을 복구하지 마십시오. 복구된 디바이스는 백업에 지정된 management center에 연결을 시도합니다.

복구는 개별적으로 그리고 로컬에서 진행됩니다.

management center 및 매니지드 디바이스에 개별적으로 및 로컬로 복원합니다. 이것은 다음을 의미합니다:

- 고가용성 또는 클러스터링 management center 또는 디바이스는 일괄 복구할 수 없습니다.
- management center를 사용하여 디바이스를 복구할 수는 없습니다. management center의 경우 웹 인터페이스를 사용하여 복구할 수 있습니다. threat defense 디바이스의 경우 SD 카드 및 재설정 버튼을 사용하는 ISA 3000 제로 터치 복원을 제외하고 threat defense CLI를 사용해야 합니다.
- management center 사용자 계정을 사용하여 매니지드 디바이스 중 하나에 로그인하고 복구할 수 없습니다. Management Center 및 디바이스는 자체 사용자 계정을 유지합니다.

Firepower 4100/9300용 구성 가져오기/내보내기 지침

구성 내보내기 기능을 사용하여 Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정을 포함하는 XML 파일을 원격 서버 또는 로컬 컴퓨터로 내보낼 수 있습니다. 나중에 해당 구성 파일을 가져와서 구성 설정을 Firepower 4100/9300 섀시에 빠르게 적용하여, 알려진 정상적인 구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다.

지침 및 제한 사항

- 구성 파일의 내용을 수정하지 마십시오. 구성 파일을 수정하면 해당 파일을 사용한 구성 가져오기가 실패할 수 있습니다.
- 애플리케이션 관련 구성 설정은 구성 파일에 포함되지 않습니다. 애플리케이션 관련 설정 및 구성을 관리하려면 애플리케이션에서 제공하는 구성 백업 도구를 사용해야 합니다.
- Firepower 4100/9300 섀시에서 설정을 가져오면 Firepower 4100/9300 섀시에 있는 모든 기존의 설정(논리적 디바이스 포함)이 삭제되고 가져오기 파일에 포함된 설정으로 완전히 교체됩니다.
- RMA 시나리오를 제외하고 설정을 내보낸 곳과 동일한 Firepower 4100/9300 섀시로 설정 파일만 가져오는 것이 좋습니다.
- 구성을 가져오는 Firepower 4100/9300 섀시의 플랫폼 소프트웨어 버전은 내보낼 때와 동일한 버전이어야 합니다. 버전이 다르면 가져오기 작업의 성공이 보장되지 않습니다. Firepower 4100/9300 섀시를 업그레이드 또는 다운그레이드할 때마다 백업 설정을 내보내는 것이 좋습니다.
- 구성을 가져오는 Firepower 4100/9300 섀시에는 내보냈을 때와 동일한 슬롯에 동일한 네트워크 모듈이 설치되어 있어야 합니다.
- 구성을 가져오는 Firepower 4100/9300 섀시에는, 가져오는 내보내기 파일에 정의된 논리적 디바이스에 대해 올바른 소프트웨어 애플리케이션 이미지가 설치되어 있어야 합니다.

- 기존 백업 파일을 덮어쓰지 않으려면, 백업 작업 시 파일 이름을 변경하거나 기존 파일을 다른 위치에 복사합니다.

참고 FXOS 가져오기/내보내기는 FXOS 구성만 백업하므로 논리적 앱을 별도로 백업해야 합니다. FXOS 구성 가져오기로 인해 논리적 디바이스가 재부팅되고 디바이스가 공장 기본 구성으로 재구축됩니다.

백업 및 복구 모범 사례

백업 및 복구에는 다음과 같은 모범 사례가 있습니다.

백업 시기

유지 보수 기간 또는 사용률이 낮은 다른 시간에 백업하는 것이 좋습니다.

시스템이 백업 데이터를 수집하는 동안 데이터 상관관계(management center만 해당) 도출이 일시적으로 일시 중지될 수 있으며, 백업 관련된 구성은 할 수 없게 됩니다. 이벤트 데이터를 포함하는 경우 eStreamer와 같은 이벤트 관련 기능을 사용할 수 없습니다.

다음 상황에서 백업해야 합니다.

- 정기 예약 백업.

  재해 복구 계획의 일환으로, 정기적인 백업 수행을 권장합니다.

  management center 설정 프로세스는 매주 설정 전용 백업을 예약하여 로컬에 저장합니다. 이는 전체 오프 사이트 백업을 대체하지 않습니다. 초기 설정이 완료되면 예약된 작업을 검토하고 조직의 요구에 맞게 조정해야 합니다. 자세한 내용은 예약 백업를 참고하십시오.

- SLR 변경 후.

  SLR(Specific Licensing Reservations)을 변경한 후 management center를 백업합니다. 변경을 수행한 다음 이전 백업을 복원할 경우, 특정 라이선싱 반환 코드에 문제가 발생하여 고아 엔타이틀먼트가 발생할 수 있습니다.

- 업그레이드 또는 이미지 재설치 전.

  업그레이드가 심각하게 실패할 경우, 이미지를 재설치하고 복구해야 할 수 있습니다. 이미지를 재설치하면 시스템 암호를 포함하여 대부분의 설정이 공장 기본값으로 돌아갑니다. 최근 백업이 있는 경우, 보다 신속하게 정상 작업으로 돌아갈 수 있습니다.

- 업그레이드 후.

  새로 업그레이드한 구축의 스냅샷을 생성할 수 있도록 업그레이드 후 백업합니다. 매니지드 디바이스를 업그레이드한 후 management center를 백업하는 것이 좋습니다. 그러면 새 management center 백업 파일이 해당 디바이스가 업그레이드되었음을 '인식'합니다.

백업 파일 보안 유지

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다.

PKI 개체의 개인 키 - 구축 지원에 필요한 공개 키 인증서 및 페어링된 개인 키가 백업되기 전에 암호 해독됨을 나타냅니다. 키는 백업을 복원할 때 임의로 생성된 키로 다시 암호화됩니다.

참고 management center와 디바이스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 로컬에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제되어 로컬에 저장된 백업을 제거할 수 있습니다.

특히 백업 파일은 암호화되지 않으므로 무단 액세스를 허용하지 않습니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

management center의 시스템 설정에서 NFS, SMB 또는 SSHFS 네트워크 볼륨을 원격 스토리지로 마운트할 수 있습니다. 이렇게 하면 모든 후속 백업이 해당 볼륨에 복사되지만, 계속해서 management center를 사용하여 백업을 관리할 수 있습니다. 자세한 내용은 원격 스토리지 디바이스 및 백업 및 원격 스토리지 관리, 31 페이지를 참조하십시오.

management center만 네트워크 볼륨을 마운트합니다. 매니지드 디바이스 백업 파일은 management center를 통해 라우팅됩니다. management center와 해당 디바이스 간에 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(문제 해결 TechNote)을 참조하십시오.

Management Center 고가용성 구축의 백업 및 복구

management center 고가용성 구축에서는 한 management center를 백업해도 다른 FMC는 백업되지 않습니다. 두 피어를 정기적으로 백업해야 합니다. 특정 HA 피어를 다른 HA 피어의 백업 파일을 사용하여 복구하지 마십시오. 백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

백업에 성공하지 않고도 HA management center를 교체할 수 있습니다. 백업 성공 여부에 관계없이 HA management center를 교체하는 방법에 대한 자세한 내용은 고가용성 쌍의 Management Center 교체의 내용을 참조하십시오.

Threat Defense 고가용성 구축의 백업 및 복구

threat defense 고가용성 구축에서는 다음을 수행해야 합니다.

- management center에서 디바이스 쌍을 백업하되, threat defense CLI에서 개별적으로 로컬에서 복구합니다.

  백업 프로세스에서는 threat defense 고가용성 디바이스용으로 고유한 백업 파일을 생성합니다. 특정 고가용성 피어를 다른 HA 피어의 백업 파일을 사용하여 복구하지 마십시오. 백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

  threat defense 고가용성 디바이스의 역할은 백업 파일 이름에 표시됩니다. 복구할 때는 적절한 백업 파일(기본 및 보조)을 선택해야 합니다.

- 복구하기 전에 고가용성을 일시 중단하거나 해제하지 마십시오.

  고가용성 설정을 유지 관리하면 복구 후 교체 디바이스를 쉽게 다시 연결할 수 있습니다. 이 작업을 수행하려면 고가용성 동기화를 다시 시작해야 합니다.

- 두 피어에서 동시에 **restore** CLI 명령을 실행하지 마십시오.

  백업이 성공했다고 가정하면 고가용성 쌍의 피어 중 하나 또는 둘 다를 교체할 수 있습니다. 동시에 수행할 수 있는 모든 물리적 교체 작업에는 랙킹 해제, 재랙킹 등이 있습니다. 그러나 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 두 번째 디바이스에서 **restore** 명령을 실행하지 마십시오.

백업에 성공하지 않고도 threat defense 고가용성 디바이스를 교체할 수 있습니다..

Threat Defense 클러스터링 구축의 백업 및 복원

threat defense 클러스터링 구축에서는 다음을 수행해야 합니다.

- management center에서 전체 클러스터를 백업하지만 threat defense CLI에서 노드를 개별적으로 로컬로 복원합니다.

  백업 프로세스는 각 클러스터 노드에 대한 고유한 백업 파일을 포함하는 번들 tar 파일을 생성합니다. 한 노드를 다른 노드의 백업 파일로 복원하지 마십시오. 백업 파일에는 디바이스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

  노드의 역할은 백업 파일 이름에 표시됩니다. 복구할 때는 적절한 백업 파일(제어 또는 데이터)을 선택해야 합니다.

  개별 노드는 백업할 수 없습니다. 데이터 노드가 백업에 실패하는 경우에도 management center는 다른 모든 노드를 백업합니다. 제어 노드가 백업에 실패하면 백업이 취소됩니다.

- 복구하기 전에 클러스터링을 일시 중단하거나 해제하지 마십시오.

  클러스터 구성을 유지 관리하면 복구 후 교체 디바이스를 쉽게 다시 연결할 수 있습니다.

- 여러 노드에서 동시에 **restore** CLI 명령을 실행하지 마십시오. 데이터 노드를 복원하기 전에 먼저 제어 노드를 복원하고 클러스터에 다시 조인할 때까지 기다리는 것이 좋습니다.

  백업에 성공한 경우 클러스터의 여러 노드를 교체할 수 있습니다. 동시에 수행할 수 있는 모든 물리적 교체 작업에는 랙킹 해제, 재랙킹 등이 있습니다. 그러나 재부팅을 포함하여 이전 노드에 대한 복구 프로세스가 완료될 때까지 추가 노드에서 **restore** 명령을 실행하지 마십시오.

Firepower 4100/9300 섀시 백업 및 복구

Firepower 4100/9300 섀시에서 threat defense 소프트웨어를 복구하려면 섀시에서 호환되는 FXOS 버전을 실행해야 합니다.

Firepower 4100/9300 섀시를 백업할 때는 FXOS 설정도 백업하는 것이 좋습니다. 추가 모범 사례는 Firepower 4100/9300용 구성 가져오기/내보내기 지침 , 5 페이지의 내용을 참조하십시오.

백업 전

백업하기 전에 다음을 수행해야 합니다.

- management center에서 VDB 및 SRU를 업데이트합니다.

  항상 최신 취약성 데이터베이스(VDB) 및 침입 규칙(SRU)을 사용하는 것이 좋습니다. management center를 백업하기 전에 Cisco 지원 및 다운로드 사이트에서 최신 버전을 확인하십시오.

- 디스크 공간을 확인합니다.

  백업을 시작하기 전에 어플라이언스 또는 원격 스토리지 서버에 충분한 디스크 공간이 있는지 확인하십시오. 사용 가능한 공간이 Backup Management(백업 관리) 페이지에 표시됩니다.

  공간이 충분하지 않으면 백업이 실패할 수 있습니다. 특히 백업을 예약하는 경우, 정기적으로 백업 파일을 정리하거나 원격 스토리지 위치에 추가 디스크 공간을 할당해야 합니다.

복구 전

복구하기 전에 다음을 수행해야 합니다.

- 라이선스 변경 사항을 되돌립니다.

  백업 이후에 수행한 라이선싱 변경 사항을 되돌립니다.

  그렇지 않으면 복구 후 라이선스 충돌 또는 고아 엔타이틀먼트가 발생할 수 있습니다. 그러나 CSSM(Cisco Smart Software Manager)에서 등록을 취소하지 마십시오. CSSM에서 등록을 취소하는 경우, 복구 후 다시 등록을 취소한 다음 재등록해야 합니다.

  복구가 완료되면 라이선싱을 다시 설정합니다. 라이선싱 충돌 또는 분리 자격이 확인되면 Cisco TAC에 문의하십시오.

- 결함이 있는 어플라이언스의 연결을 끊습니다.

  관리 인터페이스와 데이터 인터페이스(디바이스의 경우)의 연결을 끊습니다.

  threat defense 디바이스를 복구하면 교체 디바이스의 관리 IP 주소가 이전 디바이스의 관리 IP 주소로 설정됩니다. IP 충돌 방지를 위해, 교체 디바이스에 백업을 복구하기 전에 관리 네트워크와 이전 디바이스의 연결을 끊으십시오.

  management center를 복구해도 관리 IP 주소는 변경되지 않습니다. 교체 시 수동으로 설정해야 하는데, 작업 전에 네트워크에서 이전 어플라이언스의 연결을 해제해야 합니다.

- 매니지드 디바이스를 등록 취소하지 마십시오.

  management center 또는 매니지드 디바이스를 복구하든 관계없이 네트워크에서 어플라이언스의 물리적 연결을 끊더라도 management center에서 디바이스를 등록 취소하지 마십시오.

  등록을 취소한다면 보안 구역에서 인터페이스 매핑 같은 일부 디바이스 구성을 다시 설정해야 합니다. 복구 후에는 management center와 디바이스가 정상적으로 통신을 시작해야 합니다.

- 이미지 재설치.

  RMA 시나리오에서는 교체 어플라이언스가 공장 기본값으로 설정된 상태로 제공됩니다. 그러나 교체 어플라이언스가 이미 설정된 경우, 이미지를 재설치하는 것이 좋습니다. 이미지를 재설치하면 시스템 암호를 포함하여 대부분의 설정이 공장 기본값으로 돌아갑니다. 주 버전으로만 이미지를 재설치할 수 있으므로 이미지를 재설치한 후에 패치를 적용해야 할 수 있습니다.

이미지를 재설치하지 않을 경우, management center 침입 이벤트 및 파일 목록이 덮어쓰이지 않고 병합됩니다.

복원 후

복구 후 다음을 수행해야 합니다.

- 복구되지 않은 항목을 재구성합니다.

  여기에는 라이선싱, 원격 스토리지 및 감사 로그 서버 인증서 설정 재구성이 포함될 수 있습니다. 또한 실패한 threat defense VPN 인증서를 다시 추가/다시 등록해야 합니다.

- management center에서 VDB 및 SRU를 업데이트합니다.

  항상 최신 취약성 데이터베이스(VDB) 및 침입 규칙(SRU)을 사용하는 것이 좋습니다. 이는 백업의 VDB가 교체 management center의 VDB를 덮어쓰기 때문에 VDB에 특히 중요합니다.

- 구축.

  management center를 복구한 후 모든 매니지드 디바이스에 구축합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스에 기존 구성 재구축을 참조하십시오. 또는 구축해야 하는 management center 또는 디바이스를 복원하는지 여부.

Management Center 또는 매니지드 디바이스 백업

지원되는 어플라이언스에 대해 온 디맨드 또는 예약 백업을 수행할 수 있습니다.

management center에서 디바이스를 백업하는 데 백업 프로필이 필요하지 않습니다. 그러나 7000/8000 시리즈 디바이스의 로컬 백업과 마찬가지로 management center 백업에는 백업 프로파일이. 온 디맨드 백업 프로세스를 통해 새 백업 프로파일을 생성할 수 있습니다.

FMC 백업

온 디맨드 FMC 백업을 수행하려면 이 절차를 사용합니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬 및 원격으로 저장된 모든 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 기존 백업 프로파일을 사용할지 아니면 새로 시작할지를 선택합니다.

FMC 백업을 사용하려면 백업 프로파일을 사용하거나 생성해야 합니다.

- 기존 백업 프로파일을 사용하려면 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

  사용하려는 프로파일 옆에 있는 편집 아이콘을 클릭합니다. 그런 다음 **Start Backup(**백업 시작**)**을 클릭하여 지금 백업을 시작할 수 있습니다. 또는 프로파일을 편집하려면 다음 단계로 이동합니다.

- **Firepower Management Backup(Firepower** 관리 백업**)**을 클릭하여 새로 시작하고 새 백업 프로파일을 생성합니다.

  백업 프로파일의 이름을 입력합니다.

단계 **3** 백업할 항목을 선택합니다.

- 구성 백업
- 이벤트 백업
- **Threat Intelligence Director** 백업

다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는 TID 데이터만 백업할 수는 없습니다. 이러한 각 선택 항목에 대해 백업 및 백업되지 않는 항목에 대한 자세한 내용은 백업 및 복원 정보, 1 페이지의 내용을 참조하십시오.

단계 **4** FMC 백업 파일의 스토리지 위치를 적어둡니다.

이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. 자세한 내용은 백업 및 원격 스토리지 관리, 31 페이지를 참고하십시오.

단계 **5** (선택 사항) **Copy when complete(**완료 시 복사**)**를 활성화하여 완료된 FMC 백업을 원격 서버에 복사합니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

참고 이 옵션은 백업을 로컬에 저장하거나 SCP를 원격 위치에 저장하려는 경우 유용합니다. SSH 원격 스토리지를 설정한 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉터리에 백업 파일을 복사하지 마십시오.

단계 **6** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 FMC를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성

단계 **7** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

기존 백업 프로파일을 사용하지 않는 경우 시스템에서 자동으로 생성하여 사용합니다. 지금 백업을 실행하지 않으려는 경우 **Save(**저장**)** 또는 **Save As New(**새로 저장**)**를 클릭하여 프로파일을 저장할 수 있습니다. 두 경우 모두 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

단계 **8** 메시지 센터에서 진행 상황을 모니터링합니다.

시스템이 백업 데이터를 수집하는 동안 데이터 상관관계 도출이 일시적으로 일시 중지될 수 있으며, 백업 관련된 구성은 할 수 없게 됩니다. 원격 스토리지를 설정했거나 **Copy when complete(**완료시 복사**)**를 활성화한 경우 FMC가 원격 서버에 임시 파일을 쓸 수 있습니다. 이러한 파일은 백업 프로세스가 끝나면 정리됩니다.

다음에 수행할 작업

원격 스토리지를 설정했거나 **Copy when complete(**완료시 복사**)**를 활성화한 경우 백업 파일의 전송 성공을 확인합니다.

Management Center에서 디바이스 백업

이 절차를 사용하여 다음 디바이스에 대한 온 디맨드 백업을 수행합니다.

- threat defense: 물리적 디바이스, 독립형, 고가용성, 클러스터
- threat defense virtual: 프라이빗 클라우드, 독립형, 고가용성, 클러스터

백업 및 복구는 클러스터된 디바이스.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

Firepower 4100/9300 섀시를 백업하는 경우에는 FXOS구성FXOS 구성 파일 내보내기, 13 페이지도 백업하는 것이 특히 중요합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을 선택한 다음 **Managed Device Backup(**매니지드 디바이스 백업**)**을 클릭합니다.

단계 **2** 하나 이상의 **Managed Devices(**매니지드 디바이스**)**를 선택합니다.

클러스터링의 경우 클러스터를 선택합니다. 개별 노드에서는 백업을 수행할 수 없습니다.

단계 **3** 디바이스 백업 파일의 스토리지 위치를 적어 둡니다.

이는 `/var/sf/remote-backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. ISA 3000의 경우 SD 카드가 설치되어있는 경우 백업 사본이 SD 카드의 `/mnt/disk3/backup`에도 생성됩니다. 자세한 내용은 백업 및 원격 스토리지 관리, 31 페이지를 참고하십시오.

단계 **4** 원격 스토리지를 설정하지 않은 경우, **Management Center**로 검색할지 여부를 선택합니다.

- 활성화됨(기본값): `/var/sf/remote-backup/`에 있는 management center에 백업을 저장합니다.

  클러스터의 경우 이 옵션은 항상 선택되어 있습니다. 개별 노드 백업 파일은 management center에 복사된 다음 단일 압축 tar 파일로 번들된 다음 원격 스토리지에 복사됩니다.

- Disabled: `/var/sf/backup`의 디바이스에 백업을 저장합니다.

단계 **5** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

단계 **6** 메시지 센터에서 진행 상황을 모니터링합니다.

다음에 수행할 작업

원격 저장소를 구성한 경우 백업 파일이 성공적으로 전송되었는지 확인합니다.

FXOS 구성 파일 내보내기

Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정을 포함하는 XML 파일을 원격 서버 또는 로컬 컴퓨터로 내보내려면 구성 내보내기 기능을 사용합니다.

참고 이 절차에서는 위협 방어를 백업할 때 Secure Firewall 섀시 관리자을(를) 사용하여 FXOS 설정을 내보내는 방법을 설명합니다. CLI 절차는 Cisco Firepower 4100/9300 FXOS CLI 설정 가이드의 해당 버전을 참조하십시오.

시작하기 전에

Firepower 4100/9300용 구성 가져오기/내보내기 지침 을 검토합니다.

프로시저

단계 **1** Secure Firewall 섀시 관리자에서 **System(**시스템**)** > **Configuration(**설정**)** > **Export(**내보내기**)**를 선택합니다.

단계 **2** 구성 파일을 로컬 컴퓨터로 내보내려면:

a) **Local(**로컬**)**을 클릭합니다.

b) **Export(**내보내기**)**를 클릭합니다.
구성 파일이 생성되고, 브라우저에 따라 기본 다운로드 위치로 파일이 자동으로 다운로드되거나 파일을 저장하라는 프롬프트가 표시될 수 있습니다.

단계 **3** 구성 파일을 원격 서버로 내보내려면:

a) **Remote(**원격**)**를 클릭합니다.

b) 원격 서버와의 통신에서 사용할 프로토콜을 선택합니다. FTP, TFTP, SCP, SFTP 중 하나일 수 있습니다.

c) 백업 파일을 저장할 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 섀시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브, 기타 읽기/쓰기 미디어일 수 있습니다.

IP 주소가 아니라 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

d) 기본값 이외의 포트를 사용하려는 경우 **Port(**포트**)** 필드에 포트 번호를 입력합니다.

e) 시스템이 원격 서버에 로그인할 때 사용할 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

g) **Location(**위치**)** 필드에 구성 파일을 내보낼 전체 경로(파일 이름 포함)를 입력합니다.

h) 사용할 원격 구성에 대해 **Export(**내보내기**)**.
구성 파일이 생성되고 지정된 위치로 내보내기가 수행됩니다.

백업 프로파일 생성

백업 프로파일은 백업된 환경 설정 집합, 즉 백업 대상, 백업 파일을 저장할 위치 등입니다.

FMC 백업 및 7000/8000 Series 로컬 백업에는 백업 프로파일이 필요합니다. 백업 프로파일은 FMC에서 디바이스를 백업하는 데 필요하지 않습니다.

온 디맨드 FMC을 수행할 때 기존 백업 프로파일을 선택하지 않으면 시스템에서 자동으로 생성하여 사용합니다. 그런 다음 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

다음 절차에서는 온 디맨드 백업을 수행하지 않고 백업 프로필을 생성하는 방법을 설명합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**를 선택하고 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

단계 **2** **Create Profile(**프로필 생성**)**을 클릭하고 **Name(**이름**)**을 입력합니다.

단계 **3** 백업할 항목을 선택합니다.

- 구성 백업
- 이벤트 백업
- **Threat Intelligence Director** 백업

다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는 TID 데이터만 백업할 수는 없습니다. 이러한 각 선택 항목에 대해 백업 및 백업되지 않는 항목에 대한 자세한 내용은 백업 및 복원 정보, 1 페이지의 내용을 참조하십시오.

단계 **4** 백업 파일의 스토리지 위치를 적어둡니다.

이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. ISA 3000의 경우 SD 카드가 설치되어있는 경우 백업 사본이 SD 카드의 `/mnt/disk3/backup`에도 생성됩니다. 자세한 내용은 백업 및 원격 스토리지 관리, 31 페이지를 참고하십시오.

단계 **5** (선택 사항) **Copy when complete(**완료 시 복사**)**를 활성화하여 완료된 FMC 백업을 원격 서버에 복사합니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

참고 이 옵션은 백업을 로컬에 저장하거나 SCP를 원격 위치에 저장하려는 경우 유용합니다. SSHFS 원격 스토리지를 설정한 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉터리에 백업 파일을 복사하지 마십시오.

단계 **6** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 FMC를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성

단계 **7** **Save(**저장**)**를 클릭합니다.

Management Center 및 매니지드 디바이스 복원

management center 웹 인터페이스를 사용하여 백업에서 복구합니다. threat defense 디바이스의 경우 threat defense CLI를 사용해야 합니다. management center를 사용하여 디바이스를 복구할 수는 없습니다.

다음 섹션에서는 management center 및 매니지드 디바이스를 복구하는 방법을 설명합니다.

백업에서 **Management Center** 복원

management center 백업을 복구할 때 백업 파일에 포함된 구성 요소(이벤트, 설정, TID 데이터) 중 일부 또는 전체를 복구하도록 선택할 수 있습니다.

참고 설정을 복구하면 극히 드문 예외를 제외하고 모든 설정을 덮어씁니다. 또한 management center가 재부팅됩니다. 이벤트 및 TID 데이터를 복구하면 침입 이벤트를 제외한 모든 기존 이벤트 및 TID 데이터를 덮어씁니다. 준비가 되었는지 확인하십시오.

백업에서 management center를 복구하려면 이 절차를 사용합니다.management center HA 구축에서의 백업 및 복구에 대한 자세한 내용은 고가용성 쌍의 Management Center 교체의 내용을 참고하십시오.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

프로시저

단계 **1** 복구하려는 management center에 로그인합니다.

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

Backup Management(백업 관리) 페이지에는 로컬 및 원격으로 저장된 모든 백업 파일이 나열됩니다. 백업 파일을 클릭하고 내용을 확인할 수 있습니다.

백업 파일이 목록에 없고 로컬 컴퓨터에 저장한 경우 **Upload Backup(**백업 업로드**)**을 클릭합니다. 백업 및 원격 스토리지 관리, 31 페이지의 내용을 참조하십시오.

단계 **3** 복구하려는 백업 파일을 선택하고 **Restore(**복구**)**를 클릭합니다.

단계 **4** 복구할 수 있는 구성 요소 중에서 선택한 다음 **Restore(**복구**)**를 다시 클릭하여 시작합니다.

단계 **5** 메시지 센터에서 진행 상황을 모니터링합니다.

구성을 복구하는 경우, management center를 재부팅한 후 다시 로그인하면 됩니다.

다음에 수행할 작업

- 필요에 따라 복구 전에 되돌린 라이선싱 설정을 다시 구성합니다. 라이선싱 충돌 또는 분리 자격이 확인되면 Cisco TAC에 문의하십시오.
- 필요에 따라 원격 스토리지 및 감사 로그 서버 인증서 설정을 다시 구성합니다. 이러한 설정은 백업에 포함되지 않습니다.
- (선택 사항) SRU 및 VDB를 업데이트합니다. Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치하는 것이 좋습니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

백업에서 Threat Defense 복원: Firepower 1000/2100, Secure Firewall 3100, ISA 3000(비제로 터치)

Threat Defense 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

하드웨어 장애 시 이 절차에서는 Firepower 1000/2100, Secure Firewall 3100 또는 ISA 3000 threat defense 디바이스를 독립형이나 고가용성 쌍 또는 클러스터로 교체하는 방법을 설명합니다. 여기서는 교체하려는 디바이스 또는 디바이스의 백업에 액세스할 수 있다고 가정합니다. Management Center에서 디바이스 백업, 12 페이지의 내용을 참조하십시오.SD 카드를 사용하는 ISA 3000에서의 제로 터치 복원에 대해서는 백업에서 제로 터치 복원 Threat Defense: ISA 3000, 21 페이지의 내용을 참조하십시오.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

프로시저

단계 1 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco는 Portal을 반환합니다.에서 RMA 프로세스를 시작할 수 있습니다.

단계 2 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

클러스터링의 경우 노드 백업 파일은 클러스터의 단일 압축 파일(*cluster_name*.*timestamp*.**tar.gz**)에 번들로 제공됩니다. 노드를 복원하려면 먼저 개별 노드 백업 파일 (*node_name*_**control**_*timestamp*.**tar** 또는 *node_name*_**data**_*timestamp*.**tar**)을 추출해야 합니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 management center
- 원격 스토리지 위치

threat defense 고가용성 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 31 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 3 결함이 있는 디바이스를 제거(분리)합니다.

모든 인터페이스의 연결을 끊습니다. threat defense 고가용성 구축에서는 페일오버 링크가 포함됩니다. 클러스터링의 경우 클러스터 제어 링크가 포함됩니다.

사용 중인 모델의 하드웨어 설치 및 시작 가이드를 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 4 교체 디바이스를 설치하고 관리 네트워크에 연결합니다.

디바이스를 전원에 연결하고 관리 인터페이스를 관리 네트워크에 연결합니다. threat defense 고가용성 구축에서 페일오버 링크를 연결합니다. 클러스터링의 경우 클러스터 제어 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

단계 **5** (선택 사항) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치하는 것이 좋습니다.

Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드를 참조하십시오.

단계 **6** 교체 디바이스에서 초기 설정을 수행합니다.

관리자로 threat defense CLI에 액세스합니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

결함이 있는 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

사용 중인 모델에 대한 시작 가이드의 초기 설정 항목을 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 교체 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 management center 등록 프로세스를 시작합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **7** 교체 디바이스가 결함이 있는 디바이스와 동일한 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 management center에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 threat defense 패치의 버전이 동일해야 합니다. threat defense CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) management center 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) management center에서 새로 패치한 디바이스 등록을 취소합니다.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 management center에 고스트 디바이스가 등록됩니다.

단계 **8** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다. 클러스터링의 경우 기본 클러스터 번들에서 개별 노드 백업 파일을 추출했는지 확인합니다.

단계 **9** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

threat defense 고가용성 및 클러스터링 구축에서는 적절한 백업 파일(기본 대 보조 또는 제어 대 데이터)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. 모든 디바이스를 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 다음 디바이스에서 **restore** 명령을 실행하지 마십시오.

단계 **10** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 management center에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **11** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- 고가용성 동기화를 다시 시작합니다. threat defense CLI에서 `configure high-availability resume`을 입력합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 고가용성 일시 중단 또는 재개를 참조하십시오.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **12** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **13** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업에서 제로 터치 복원 Threat Defense: ISA 3000

Threat Defense 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

하드웨어 장애 시 이 절차에서는 ISA 3000 threat defense 디바이스를 독립형 또는 HA 쌍으로 교체하는 방법을 간략하게 설명합니다. 장애가 발생한 유닛의 백업이 SD 카드에 있다고 가정합니다. Management Center에서 디바이스 백업, 12 페이지의 내용을 참조하십시오.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

프로시저

단계 1 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco는 Portal을 반환합니다.에서 RMA 프로세스를 시작할 수 있습니다.

단계 2 결함이 있는 디바이스에서 SD 카드를 제거하고 디바이스를 랙에서 분리합니다.

모든 인터페이스의 연결을 끊습니다. threat defense HA 구축에서는 페일오버 링크가 포함됩니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 3 교체 디바이스를 다시 랙킹하고 관리 네트워크에 연결합니다. threat defense HA 구축에서는 페일오버 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

디바이스 이미지를 재설치하거나 소프트웨어 패치를 적용해야 하는 경우, 전원 커넥터를 연결합니다.

단계 **4** (필요할 수 있음) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치해야 합니다. https://www.cisco.com/go/isa3000-software에서 설치 프로그램을 가져옵니다.

이미지를 재설치하려면 Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드의 내용을 참조하십시오.

단계 **5** (필요할 수 있음) 교체 디바이스가 결함이 있는 디바이스와 동일한 Firepower 소프트웨어 버전(동일한 패치 버전 포함)을 실행 중인지 확인합니다. 디바이스를 패치해야하는 경우 Secure Firewall device manager(device manager)에 연결하여 패치를 설치할 수 있습니다.

다음 절차에서는 공장 기본 구성이 있다고 가정합니다. 디바이스를 이미 구성한 경우 device manager에 로그인하여 **Device(**디바이스**)** > **Upgrades(**업그레이드**)** 페이지로 직접 이동한 후 패치를 설치할 수 있습니다.

어느 경우든 패치 패키지를 https://www.cisco.com/go/isa3000-software에서 구합니다.

a) 컴퓨터를 내부(이더넷 1/2) 인터페이스에 직접 연결하고 기본 IP 주소(**https://192.168.95.1**)에서 device manager에 액세스합니다.
b) **admin** 사용자 이름과 비밀번호 **Admin123**을 입력하고 **Login(**로그인**)**을 클릭합니다.
c) 설정 마법사를 완료합니다. device manager에서 구성한 내용은 유지하지 않습니다. 패치를 적용할 수 있도록 초기 구성을 통과하기만 하면 되므로 설정 마법사에서 입력하는 내용은 중요하지 않습니다.
d) **Device(**디바이스**)** > **Upgrades(**업그레이드**)** 페이지로 이동합니다.

   System Upgrade(시스템 업그레이드**)** 섹션에는 현재 실행 중인 소프트웨어 버전이 표시됩니다.

e) **Browse(**찾아보기**)**를 클릭하여 패치 파일을 업로드합니다.
f) **Install(**설치**)**을 클릭하여 설치 프로세스를 시작합니다.

   아이콘 옆의 정보는 디바이스가 설치 중에 재부팅되는지 여부를 나타냅니다. 디바이스가 재부팅되면 시스템에서 자동으로 로그아웃됩니다. 설치에는 30분 이상 소요될 수 있습니다.

   이 시간 동안 기다렸다가 시스템에 다시 로그인하십시오. 디바이스 요약 또는 시스템 모니터링 대시보드에 새 버전이 표시됩니다.

   참고 브라우저 창을 그냥 새로 고치지 말고, URL의 경로를 삭제한 다음 홈페이지에 다시 연결하십시오. 이렇게 하면 캐시된 정보가 최신 코드로 새로고침됩니다.

단계 **6** 교체 디바이스에 SD 카드를 삽입합니다.

단계 **7** 디바이스의 전원을 켜거나 재부팅하고 부팅을 시작한 직후 Reset(재설정) 버튼을 3초 이상 15초 이하로 길게 누릅니다.

패치를 설치하는 데 device manager를 사용한 경우 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Reboot/Shutdown(**재부팅/종료**)** 페이지에서 재부팅할 수 있습니다. threat defense CLI에서는 **reboot** 명령을 사용하십시오. 아직 전원을 연결하지 않은 경우 지금 연결합니다.

와이어 게이지 0.033인치 이하의 표준 사이즈 #1 용지 클립을 사용하여 Reset(재설정) 버튼을 누릅니다. 복원 프로세스는 부팅 중에 트리거됩니다. 디바이스가 구성을 복원한 다음 재부팅합니다. 그러면 디바이스가 management center에 자동으로 등록됩니다.

HA 쌍의 두 디바이스를 모두 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복원 프로세스가 완료될 때까지 두 번째 디바이스를 복원하지 마십시오.

단계 **8** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

현재 디바이스가 오래된 것으로 표시됩니다.

단계 **9** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- 고가용성 동기화를 다시 시작합니다. threat defense CLI에서 `configure high-availability resume`을 입력합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 고가용성 일시 중단 또는 재개를 참조하십시오.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **10** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **11** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업에서 Threat Defense 복원: Firepower 4100/9300 새시

Threat Defense 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

이 절차에서는 하드웨어 장애가 발생한 경우 Firepower 4100/9300, 독립형, 고가용성 쌍 또는 클러스터로 교체하는 방법을 간략하게 설명합니다. 다음의 백업에 액세스할 수 있다고 가정합니다.

- 논리적 디바이스 또는 하나 이상의 디바이스를 교체합니다. Management Center에서 디바이스 백업, 12 페이지의 내용을 참조하십시오.
- FXOS 설정. FXOS 구성 파일 내보내기, 13 페이지의 내용을 참조하십시오.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

프로시저

단계 **1** 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco는 Portal을 반환합니다.에서 RMA 프로세스를 시작할 수 있습니다.

단계 **2** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

클러스터링의 경우 노드 백업 파일은 클러스터의 단일 압축 파일(*cluster_name*.*timestamp*.**tar.gz**)에 번들로 제공됩니다. 노드를 복원하려면 먼저 개별 노드 백업 파일 (*node_name*_**control**_*timestamp*.**tar** 또는 *node_name*_**data**_*timestamp*.**tar**)을 추출해야 합니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 management center
- 원격 스토리지 위치

threat defense 고가용성 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 31 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **3** FXOS 설정의 성공적인 백업을 찾습니다.

단계 **4** 결함이 있는 디바이스를 제거(분리)합니다.

모든 인터페이스의 연결을 끊습니다. threat defense 고가용성 구축에서는 페일오버 링크가 포함됩니다. 클러스터링의 경우 클러스터 제어 링크가 포함됩니다.

사용 중인 모델의 하드웨어 설치 및 시작 가이드를 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 **5** 교체 디바이스를 설치하고 관리 네트워크에 연결합니다.

디바이스를 전원에 연결하고 관리 인터페이스를 관리 네트워크에 연결합니다. threat defense 고가용성 구축에서 페일오버 링크를 연결합니다. 클러스터링의 경우 클러스터 제어 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

단계 **6** (선택 사항) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치하는 것이 좋습니다.

해당 Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 설정 가이드에서 공장 기본 설정 복구에 대한 지침을 참조하십시오.

단계 **7** FXOS가 호환되는 버전을 실행 중인지 확인합니다.

논리적 디바이스를 다시 추가하기 전에 호환되는 FXOS 버전을 실행 중이어야 합니다. 섀시 관리자를 사용하여 백업된 FXOS 설정을 가져올 수 있습니다.구성 파일 가져오기, 27 페이지

단계 **8** 섀시 관리자를 사용하여 논리적 디바이스를 추가하고 초기 설정을 수행합니다.

결함이 있는 섀시의 논리적 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 논리적 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

사용 중인 모델의 시작 설명서에서 management center 구축 장을 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 논리적 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 management center에 등록합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **9** 교체 디바이스가 결함이 있는 디바이스와 동일한 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 management center에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 threat defense 패치의 버전이 동일해야 합니다. threat defense CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) management center 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) management center에서 새로 패치한 디바이스 등록을 취소합니다.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 management center에 고스트 디바이스가 등록됩니다.

단계 **10** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다. 클러스터링의 경우 기본 클러스터 번들에서 개별 노드 백업 파일을 추출했는지 확인합니다.

단계 **11** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

threat defense 고가용성 및 클러스터링 구축에서는 적절한 백업 파일(기본 대 보조 또는 제어 대 데이터)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. 모든 디바이스를 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 다음 디바이스에서 **restore** 명령을 실행하지 마십시오.

단계 **12** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 management center에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **13** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.

- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **14** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **15** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

구성 파일 가져오기

Firepower 4100/9300 섀시에서 전에 내보낸 구성 설정을 적용하려면 구성 가져오기 기능을 사용할 수 있습니다. 이 기능을 사용하면 알려진 양호한 구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다.

참고 이 절차에서는 소프트웨어를 복구하기 전에 섀시 관리자을(를) 사용하여 FXOS 설정을 가져오는 방법을 설명합니다. CLI 절차는 Cisco Firepower 4100/9300 FXOS CLI 설정 가이드의 해당 버전을 참조하십시오.

시작하기 전에

Firepower 4100/9300용 구성 가져오기/내보내기 지침 을 검토합니다.

프로시저

단계 **1** 섀시 관리자에서 **System(**시스템**)** > **Tools(**도구**)** > **Import(**가져오기/내보내기**)**를 선택합니다.

단계 **2** 로컬 구성 파일로부터 가져오려면:

a) **Local(**로컬**)**을 클릭합니다.

b) **Choose File(**파일 선택**)**을 클릭하고 가져올 구성 파일을 찾아 선택합니다.

c) **Import(**가져오기**)**를 클릭합니다.
확인 대화 상자가 열리면서 계속 진행할 것인지를 물어보고 섀시를 재시작해야 한다고 경고합니다.

d) **Yes(**예**)**를 클릭하여 지정된 구성 파일을 가져올 것임을 확인합니다.
기존의 구성이 삭제되고, 가져오기 파일에 지정된 구성이 Firepower 4100/9300 섀시에 적용됩니다. 가져오는 동안 Breakout 포트 구성이 변경되는 경우 Firepower 4100/9300 섀시를 다시 시작해야 합니다.

단계 **3** 원격 서버에 있는 구성 파일로부터 가져오려면:

a) **Remote(**원격**)**를 클릭합니다.
b) 원격 서버와의 통신에서 사용할 프로토콜을 선택합니다. FTP, TFTP, SCP, SFTP 중 하나일 수 있습니다.
c) 기본값 이외의 포트를 사용하려는 경우 **Port(**포트**)** 필드에 포트 번호를 입력합니다.
d) 백업 파일을 저장할 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 섀시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브, 기타 읽기/쓰기 미디어일 수 있습니다.

   IP 주소가 아니라 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

e) 시스템이 원격 서버에 로그인할 때 사용할 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
g) **File Path(**파일 경로**)** 필드에 설정 파일의 전체 경로(파일 이름 포함)를 입력합니다.
h) 사용할 원격 구성에 대해 **Import(**가져오기**)**.
확인 대화 상자가 열리면서 계속 진행할 것인지를 물어보고 섀시를 재시작해야 한다고 경고합니다.
i) **Yes(**예**)**를 클릭하여 지정된 구성 파일을 가져올 것임을 확인합니다.
기존의 구성이 삭제되고, 가져오기 파일에 지정된 구성이 Firepower 4100/9300 섀시에 적용됩니다. 가져오는 동안 Breakout 포트 구성이 변경되는 경우 Firepower 4100/9300 섀시를 다시 시작해야 합니다.

백업에서 **Threat Defense** 복원**: Threat Defense Virtual**

프라이빗 클라우드, 독립형, 고가용성 쌍 또는 클러스터에서 결함이 있거나 장애가 발생한 threat defense virtual 디바이스를 교체하려면 이 절차를 사용합니다.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 3 페이지
- 백업 및 복원 지침 및 제한 사항, 4 페이지
- 백업 및 복구 모범 사례, 6 페이지

프로시저

단계 **1** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

클러스터링의 경우 노드 백업 파일은 클러스터의 단일 압축 파일(*cluster_name*.*timestamp*.**tar.gz**)에 번들로 제공됩니다. 노드를 복원하려면 먼저 개별 노드 백업 파일 (*node_name*_**control**_*timestamp*.**tar** 또는 *node_name*_**data**_*timestamp*.**tar**)을 추출해야 합니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 management center
- 원격 스토리지 위치

threat defense 고가용성 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 31 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **2** 결함이 있는 디바이스를 제거합니다.

가상 시스템을 종료, 전원 끄기 및 삭제합니다. 절차는 가상 환경을 위한 설명서를 참조하십시오.

단계 **3** 교체 디바이스를 구축합니다.

단계 **4** 교체 디바이스에서 초기 설정을 수행합니다.

콘솔을 사용하여 관리자로 threat defense CLI에 액세스합니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

결함이 있는 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

참고 교체 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 management center 등록 프로세스를 시작합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **5** 교체 디바이스가 결함이 있는 디바이스와 동일한 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 management center에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 threat defense 패치의 버전이 동일해야 합니다. threat defense CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) management center 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) management center에서 새로 패치한 디바이스 등록을 취소합니다.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 management center에 고스트 디바이스가 등록됩니다.

단계 **6** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다. 클러스터링의 경우 기본 클러스터 번들에서 개별 노드 백업 파일을 추출했는지 확인합니다.

단계 **7** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

threat defense 고가용성 및 클러스터링 구축에서는 적절한 백업 파일(기본 대 보조 또는 제어 대 데이터)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. 모든 디바이스를 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 다음 디바이스에서 **restore** 명령을 실행하지 마십시오.

단계 **8** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 management center에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **9** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.

- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **10** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **11** 데이터 인터페이스를 추가 및 설정합니다.

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업 및 원격 스토리지 관리

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다. 파일 이름에는 다음을 포함할 수 있는 식별 정보가 포함됩니다.

- 백업 프로파일 또는 백업과 연결된 예약된 작업의 이름입니다.
- 백업된 어플라이언스의 표시 이름 또는 IP 주소입니다.
- 어플라이언스의 역할(예: HA 쌍의 멤버).

어플라이언스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 어플라이언스에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제될 수 있습니다. 업그레이드는 로컬에 저장된 백업을 제거합니다. 옵션에 대한 자세한 내용은 백업 스토리지 위치, 33 페이지의 내용을 참조하십시오.

주의 특히 백업 파일은 암호화되지 않으므로 무단 액세스를 허용하지 않습니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

다음 절차에서는 백업 파일을 관리하는 방법을 설명합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에 사용 가능한 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 다음 중 하나를 수행합니다.

표 ***1:*** 원격 스토리지 및 백업 파일 관리

변경 후	수행해야 할 작업
FMC 시스템 설정을 편집할 필요 없이 백업을 위한 원격 스토리지를 활성화하거나 비활성화합니다.	**Enable Remote Storage for Backups(**백업에 원격 스토리지 활성화**)**를 클릭합니다. 이 옵션은 원격 스토리지를 설정한 후에만 나타납니다. 여기에서 토글하면 시스템 설정 (**System(**시스템**) > Configuration(**설정**) > Remote Storage Device(**원격 스토리지 디바이스**))**에서도 토글됩니다. 팁 원격 스토리지 설정에 빠르게 액세스하려면 Backup Management(백업 관리) 페이지의 오른쪽 위에 있는 **Remote Storage(**원격 스토리지**)**를 클릭합니다. 참고 원격 스토리지 위치에 백업을 저장하려면 Retrieve to Management Center(Management Center로 검색) 옵션도 활성화해야 합니다(참조).Management Center에서 디바이스 백업, 12 페이지
FMC와 원격 스토리지 위치 간에 파일을 이동합니다.	**Move(**이동**)**를 클릭합니다. 원하는 만큼 파일을 앞뒤로 이동할 수 있습니다. 이렇게 하면 현재 위치에서 파일이 복사되지 않고 삭제됩니다. 백업 파일을 원격 스토리지에서 FMC로 이동할 때 FMC에 저장되는 위치는 백업의 종류에 따라 달라집니다. • FMC 백업: `/var/sf/backup` • 디바이스 백업: `/var/sf/remote-backup`
백업의 내용을 봅니다.	백업 파일을 클릭합니다.
백업 파일을 삭제합니다.	백업 파일을 선택하고 **Delete(**삭제**)**를 클릭합니다. 로컬 및 원격에 저장된 백업 파일을 모두 삭제할 수 있습니다.
컴퓨터에서 연락처 파일을 업로드합니다.	**Upload Backup(**백업 업로드**)**을 클릭하고 백업 파일을 선택한 다음 **Upload Backup(**백업 업로드**)**을 다시 클릭합니다.
백업을 컴퓨터에 다운로드합니다.	백업 파일을 선택하고 **Download(**다운로드**)**를 클릭합니다. 백업 파일을 이동하는 것과 달리 FMC에서 백업을 삭제하지 않습니다.

백업 스토리지 위치

다음 표에서는 management center 및 매니지드 디바이스의 백업 스토리지 옵션에 대해 설명합니다.

표 *2:* 백업 스토리지 위치

위치	세부 정보
원격(네트워크 볼륨(NFS, SMB, SSHFS) 마운트를 통해)	참고 원격 스토리지를 구성하고 **Retrieve to Management Center(**관리 센터로 검색**)** 옵션을 활성화한 경우에만 원격 스토리지 위치에 백업이 저장됩니다(Management Center에서 디바이스 백업, 12 페이지 참조). management center의 시스템 설정에서 NFS, SMB 또는 SSHFS 네트워크 볼륨을 management center 및 디바이스 백업용 원격 스토리지로 마운트할 수 있습니다. 원격 스토리지 디바이스의 내용을 참조하십시오.) 이렇게 하면 모든 후속 management center 백업 및 *management center*시작 디바이스 백업이 해당 볼륨에 복사되지만, 계속해서 management center를 사용하여 관리할 수 있습니다(복구, 다운로드, 업로드, 삭제, 이동). management center만 네트워크 볼륨을 마운트합니다. 매니지드 디바이스 백업 파일은 management center를 통해 라우팅됩니다. management center와 해당 디바이스 간에 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(문제 해결 TechNote)을 참조하십시오.

위치	세부 정보
원격(복사를 통해)(SCP)	참고 원격 스토리지를 구성하고 **Retrieve to Management Center(**관리 센터로 검색**)** 옵션을 활성화한 경우에만 원격 스토리지 위치에 백업이 저장됩니다(Management Center에서 디바이스 백업, 12 페이지 참조). management center의 경우, **Copy when complete(**완료 시 복사**)** 옵션을 사용하여 완료된 백업을 원격 서버에 안전하게 복사(SCP)할 수 있습니다. 네트워크 볼륨을 마운트하여 원격 스토리지와 비교할 때 **Copy when complete(**완료 시 복사**)**는 NFS 또는 SMB 볼륨에 복사할 수 없습니다. CLI 옵션을 제공하거나 디스크 공간 임계값을 설정할 수 없으며, 보고서의 원격 스토리지에는 영향을 주지 않습니다. 또한 백업 파일을 복사한 후에는 관리할 수 없습니다. 이 옵션은 백업을 로컬에 저장하고 SCP를 원격 위치에 저장하려는 경우 유용합니다. 참고 management center 시스템 설정에서 SSHFS 원격 스토리지를 설정하는 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉토리에 백업 파일을 복사하지 마십시오.
로컬, management center에 있음.	네트워크 볼륨을 마운트하여 원격 스토리지를 설정하지 않은 경우, management center에 백업 파일을 저장할 수 있습니다. • management center 백업은 `/var/sf/backup`에 저장됩니다. • 백업을 수행할 때 **Retrieve to Management Center(**관리 센터로 가져오기**)** 옵션을 활성화하면 디바이스 백업이 management center의 `/var/sf/remote-backup`에 저장됩니다.
로컬, 디바이스 내부 플래시 메모리.	디바이스 백업 파일은 다음의 경우 디바이스의 `/var/sf/backup`에 저장됩니다. • 네트워크 볼륨을 마운트하여 원격 스토리지를 설정하지 마십시오. • **Retrieve to Management Center(Management Center**로 검색**)**를 활성화하지 마십시오.
로컬, 디바이스 SD 카드.	ISA 3000의 경우, 디바이스를 로컬 `/var/sf/backup` 내부 플래시 메모리 위치에 백업할 때 SD 카드가 설치되어 있으면 제로 터치 복원에 사용할 수 있도록 백업이 `/mnt/disk3/backup/`에 있는 SD 카드에 자동으로 복사됩니다.

백업 및 복원 기록

기능	버전	세부정보
클러스터의 백업 및 복원 지원	7.3	이제 management center를 사용하여 클러스터의 백업을 수행할 수 있습니다. 클러스터 노드를 복원하려면 디바이스 CLI를 사용해야 합니다. 신규/수정된 화면: **System(**시스템**)** > **Tools(**도구**)** > **Backup/Restore(**백업/복원**)** > **Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 명령: **restore remote-manager-backup** 참고 가상 방화벽의 경우 클러스터의 백업 및 복원은 VMware에서만 지원됩니다.
SD 카드를 사용한 ISA 3000의 제로 터치 복구	7.0	로컬 백업을 수행하면 백업 파일이 SD 카드에 복사됩니다(있는 경우). 교체 디바이스에서 구성을 복원하려면 새 디바이스에 SD 카드를 설치하고 디바이스가 부팅되는 동안 Reset(재설정) 버튼을 3~15초 동안 누릅니다.
threat defense 컨테이너 인스턴스의 백업 및 복원 지원	6.7	이제 management center를 사용하여 Firepower 4100/9300에서 threat defense 컨테이너 인스턴스의 온디맨드 원격 백업을 수행할 수 있습니다.
복원을 위한 VDB 요구 사항	6.6	백업에서 management center를 복원하면 기존 VDB가 백업 파일의 VDB로 대체됩니다. 복원하기 전에 VDB 버전을 더 이상 일치시킬 필요가 없습니다.
자동으로 예약된 백업	6.5	신규 또는 이미지가 재설치된 management center의 경우, 설정 프로세스는 management center 구성을 백업하고 로컬에 저장하기 위해 매주 예약된 작업을 생성합니다.
매니지드 디바이스의 온디맨드 원격 백업	6.3	이제 management center를 사용하여 특정 매니지드 디바이스의 온디맨드 원격 백업을 수행할 수 있습니다. 지원되는 플랫폼은 백업 및 복구 요구 사항, 3 페이지의 내용을 참고하십시오. 신규/수정된 화면: **System(**시스템**) > Tools(**도구**) > Backup/Restore(**백업/복원**) > Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 threat defense CLI 명령: **restore**