백업/복구

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

여러 Secure Firewall Threat Defense 디바이스에 대한 온디맨드 백업을 수행할 수 있습니다.

참고 threat defense HA 쌍에서는 온디맨드 백업이 지원되지 않습니다.

자세한 내용은 매니지드 디바이스 백업, 6 페이지를 참고하십시오.

백업 파일 저장

로컬로만 백업을 저장할 수 있습니다. threat defense 디바이스를 안전한 원격 위치에 백업하는 기능은 지원되지 않습니다.

자세한 내용은 매니지드 디바이스 백업, 6 페이지을 참고하십시오.

매니지드 디바이스 복원

threat defense 디바이스를 복구하려면 threat defense CLI를 사용해야 합니다.

자세한 내용은 CDO 매니지드 디바이스 복원, 8 페이지를 참고하십시오.

백업이란**?**

디바이스 백업은 항상 설정 전용입니다.

복구되는 항목

설정을 복구하면 드문 예외를 제외하고 모든 백업된 설정을 덮어씁니다. CDO에서 이벤트 및 TID(Threat Intelligence Director) 데이터를 복원하면 침입 이벤트를 제외한 모든 기존 이벤트 및 TID 데이터를 덮어씁니다.

다음 사항을 이해하고 계획해야 합니다.

- 백업되지 않은 항목은 복구할 수 없습니다.
- 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.

백업 및 복구 요구 사항

백업 및 복구에는 다음 요구 사항이 있습니다.

모델 요구 사항**:** 백업

다음을 백업할 수 있습니다.

- Threat Defense 독립형 디바이스, 네이티브 인스턴스, 컨테이너 인스턴스, HA 쌍
- VMware 디바이스용Threat Defense Virtual(독립형 또는 HA 쌍)

백업은 다음에 대해 지원되지 않습니다.

- Threat Defense 클러스터
- VMware용 이외의 Threat Defense Virtual 구현

백업 및 복구가 지원되지 않는 디바이스를 교체해야 한다면 디바이스별 설정을 수동으로 다시 생성해야 합니다.

모델 요구 사항**:** 복구

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

버전 요구 사항

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

라이선스 요건

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

도메인 요구 사항

수신:

- 디바이스 복구 : 없음. 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.

⚠

주의 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸 액세스에 액세스할 수 있으며, 이로 인해 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- TAC 감독하에 있거나 Firepower 및 CDO 사용자 설명서에서 명시적으로 지시한 경우에만 Linux 셸을 사용하십시오.
- Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.

재해 복구/반품 자료 인증을 위한 백업 및 복원

백업 및 복원은 주로 RMA(Return Material Authorization) 시나리오를 위한 것입니다. 결함이 있거나 고장난 물리적 어플라이언스의 복원 프로세스를 시작하기 전에, 연락해 교체 하드웨어를 요청하십시오.

백업 및 복원을 사용하여 관리 센터 간에 구성 및 이벤트를 마이그레이션할 수도 있습니다. 따라서 조직의 성장, 물리적 구현에서 가상 구현으로의 마이그레이션, 하드웨어 새로 고침 등의 기술적 또는 비즈니스적 이유로 인해 관리 센터를 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 CDO에 연결하는 데 필요한 모든 정보가 포함됩니다. 다른 관리자에서 매니지드 디바이스에 FTD 백업을 복구하지 마십시오. 복구된 디바이스는 백업에 지정된 관리자에 연결을 시도합니다.

복구는 개별적으로 그리고 로컬에서 진행됩니다.

위협 방어 디바이스에 개별적으로 및 로컬로 복원합니다. 이것은 다음을 의미합니다:

- HA(고가용성) 디바이스는 일괄 복구할 수 없습니다. 이 가이드의 복구 절차에서는 HA 환경에서 복구하는 방법을 설명합니다.
- CDO를 사용하여 디바이스를 복원할 수 없습니다. 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 수는 없습니다. management center 및 threat defense 디바이스는 고유한 사용자 계정을 유지 관리합니다.

백업 및 복원을 위한 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(FMC만 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.

- 업그레이드 또는 이미지 재설치 전.

  업그레이드가 심각하게 실패할 경우, 이미지를 재설치하고 복구해야 할 수 있습니다. 이미지 재설치는 시스템 비밀번호를 포함하여 대부분의 설정을 공장 기본값으로 되돌립니다. 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 FMC를 백업하는 것이 좋습니다. 그러면 새 FMC 백업 파일이 해당 디바이스가 업그레이드되었음을 '인식'합니다.

백업 파일 보안 유지

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다.

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

Threat Defense 고가용성 구축의 백업 및 복구

threat defense HA 구축에서는 다음을 수행해야 합니다.

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

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

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

- 복구하기 전에 HA를 일시 중단하거나 해제하지 마십시오.

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

- 두 피어에서 동시에 restore CLI 명령을 실행하지 마십시오.

  백업이 성공했다고 가정하면 HA 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.

백업 전

백업하기 전에 다음을 수행해야 합니다.

- 디스크 공간을 확인합니다.

  백업을 시작하기 전에 어플라이언스에 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 주소 충돌 방지를 위해, 교체 디바이스에 백업을 복구하기 전에 관리 네트워크와 이전 디바이스의 연결을 끊으십시오.

- 매니지드 디바이스를 등록 취소하지 마십시오.

  매니지드 디바이스를 복구하든 관계없이 네트워크에서 어플라이언스의 물리적 연결을 끊더라도 CDO에서 디바이스를 등록 취소하지 마십시오.

  등록을 취소한다면 보안 구역에서 인터페이스 매핑 같은 일부 디바이스 구성을 다시 설정해야 합니다. 복구 후에는 CDO와 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, CDO 침입 이벤트 및 파일 목록이 덮어쓰이지 않고 병합됩니다.

복원 후

복구하기 전에 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.

- 구축.

  디바이스를 복구한 후 해당 디바이스에 구축합니다. 반드시 구축해야 합니다. 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제 구축합니다.

매니지드 디바이스 백업

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

CDO를 사용하여 디바이스를 백업하는 데는 백업 프로파일이 필요하지 않습니다.

자세한 정보는 FMC에서 위협 방어 디바이스 백업, 6 페이지의 내용을 참고하십시오.

FMC에서 위협 방어 디바이스 백업

이 절차를 사용하여 다음 디바이스에 대한 온 디맨드 백업을 수행합니다.

- Threat Defense: 물리적 디바이스, 독립형, HA

- Threat Defense Virtual: VMware, 독립형, HA

백업 및 복구는 다른 플랫폼 또는 구성에 대해서는 지원되지 않습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 모든 단계를 건너뛰거나 보안 문제를 무시하지 마십시오. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 2 페이지
- 백업 및 복원 지침 및 제한 사항, 3 페이지
- 백업 및 복원을 위한 모범 사례, 4 페이지

주의 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸 액세스에 액세스할 수 있으며, 이로 인해 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- TAC 감독하에 있거나 Firepower 및 CDO 사용자 설명서에서 명시적으로 지시한 경우에만 Linux 셸을 사용하십시오.
- Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 탐색합니다.

단계 **3** Actions(작업) 창에서 **Monitoring(**모니터링**)**로 이동합니다.

단계 **4** 시스템 ( )를 선택한 다음 **Managed Device Backup(**매니지드 디바이스 백업**)**을 클릭합니다..

단계 **5** **Managed Device Backup(**매니지드 디바이스 백업**)**을 클릭합니다.

단계 **6** **Managed Devices(**매니지드 디바이스**)**에서 하나 이상의 위협 방어 디바이스를 선택합니다.

단계 **7** 디바이스 백업 파일의 스토리지 위치는 `/var/sf/remote-backup/`의 로컬 스토리지입니다.

단계 **8** 원격 스토리지를 설정하지 않은 경우, **Management Center**로 검색할지 여부를 선택합니다.

- Enabled(활성화됨)(기본값): `/var/sf/remote-backup/`에 있는 FMC에 백업을 저장합니다.
- Disabled(비활성화됨)(기본값): `/var/sf/backup`의 디바이스에 백업을 저장합니다.

단계 **9** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

단계 **10** **Notifications(**알림**)** 창의 **Tasks(**작업**)** 아래에서 진행 상황을 모니터링합니다.

CDO 매니지드 디바이스 복원

threat defense 디바이스의 경우 threat defense CLI를 사용하여 백업에서 복원해야 합니다. management center를 사용하여 디바이스를 복구할 수는 없습니다.

다음 섹션에서는 매니지드 디바이스를 복구하는 방법을 설명합니다.

- Threat Defense 디바이스 복구, 8 페이지
- 백업에서 Threat Defense 복원: Threat Defense 가상, 11 페이지

Threat Defense 디바이스 복구

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

하드웨어 장애 시 이 절차에서는 방화벽 디바이스를 독립형 또는 HA 쌍으로 교체하는 방법을 간략하게 설명합니다. 여기서는 교체하려는 디바이스 또는 디바이스의 백업에 액세스할 수 있다고 가정합니다.

threat defense HA 구축에서는 이 절차를 사용하여 피어 중 하나 또는 둘 다를 교체할 수 있습니다. 둘을 모두 교체하려면 restore CLI 명령을 제외한 두 디바이스에서 모든 단계를 동시에 수행합니다. 백업에 성공하지 않고도 threat defense HA를 교체할 수 있습니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 CDO에서 등록을 취소하지 마십시오. threat defense HA 구축에서는 HA를 일시 중단하거나 해제하지 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. 모든 단계를 건너뛰거나 보안 문제를 무시하지 마십시오. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 2 페이지
- 백업 및 복원 지침 및 제한 사항, 3 페이지
- 백업 및 복원을 위한 모범 사례, 4 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** **System(**시스템**)(⚙) > Tools(**툴**) > Backup/Restore(**백업/복원**)**로 이동합니다.

단계 **3** **Backup Management(**백업 관리**)**의 **Device Backups(**디바이스 백업**)**에서 결함 있는 디바이스의 성공적인 백업을 찾습니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- 결함이 있는 디바이스에서 `/var/sf/backup`의 FMC에 백업을 저장합니다.
- 관리 센터에서는 `/var/sf/remote-backup/`의 디바이스에 백업을 저장합니다.

threat defense HA 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서는 페어의 각 디바이스에 대해 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.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 secure copy (SCP) 명령을 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **4** 결함이 있는 디바이스를 제거(랙 해제)하고 모든 인터페이스를 분리합니다. 위협 방어 HA 구축에서는 페일오버 링크가 포함됩니다.

사용 중인 모델에 대한 하드웨어 설치 및 시작 가이드: Cisco Firepower NGFW: 설치 및 업그레이드 가이드를 참조하십시오.

참고 네트워크에서 디바이스의 연결을 끊을 때도 관리 센터에서 등록을 취소하지 마십시오. 위협 방어 HA 구축에서는 HA를 일시 중단하거나 해제하지 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. 위협 방어 HA 구축에서는 페일오버 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드: Cisco Firepower NGFW: 설치 및 업그레이드 가이드를 참조하십시오.

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.

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

단계 **7** 교체 디바이스에서 초기 설정을 수행합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 공장 기본 관리 인터페이스 IP 주소(192.168.45.45)에 SSH를 통해 연결할 수 있습니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

사용 중인 모델에 대한 시작 가이드의 초기 설정 항목인 Cisco Firepower NGFW: 설치 및 업그레이드 가이드을 참조하십시오.

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

단계 **8** 교체 디바이스가 결함이 있는 디바이스와 동일한 방화벽 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 관리 센터에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 위협 방어 패치의 버전이 동일해야 합니다. 위협 방어 CLI에는 upgrade 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) 관리 센터 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다. Cisco Secure Firewall Management Center 디바이스 설정 가이드의 *Management Center*에 디바이스 추가를 참조하십시오.

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 Firewall Management Center 업그레이드 설명서.

c) 관리 센터에서 새로 패치된 디바이스 등록 취소: Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Management Center*에서 디바이스 삭제를 참조하십시오.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 관리 센터에 고스트 디바이스가 등록됩니다.

단계 **9** 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.

단계 **10** FTD 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**

단계 **11** CDO에 로그인하고 디바이스가 연결될 때까지 기다립니다.

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

현재 디바이스가 오래된 것으로 표시됩니다.

단계 **12** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의하십시오.
- HA 동기화를 다시 시작합니다.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 FTD 디바이스에서 VPN 인증서를 제거합니다.

단계 **13** 설정을 구축합니다.

반드시 구축해야 합니다. 복구된 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제로 구축합니다.

단계 **14** 디바이스의 데이터 인터페이스를 연결합니다.

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

백업에서 **Threat Defense** 복원: **Threat Defense** 가상

결함이 있거나 실패한 VMware용 threat defense virtual 디바이스를 교체하려면 이 절차를 사용합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. 등록을 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 모든 단계를 건너뛰거나 보안 문제를 무시하지 마십시오. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 2 페이지
- 백업 및 복원 지침 및 제한 사항, 3 페이지
- 백업 및 복원을 위한 모범 사례, 4 페이지

프로시저

단계 **1** **System**(시스템)(⚙) > **Tools**(툴) > **Backup/Restore**(백업/복원)로 이동합니다.

단계 **2** **Backup Management**(백업 관리)의 **Device Backups**(디바이스 백업)에서 결함 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.

- 결함이 있는 디바이스에서 `/var/sf/backup`의 CDO에 백업을 저장합니다.
- management center에서는 `/var/sf/remote-backup/`의 디바이스에 백업을 저장합니다.

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.

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 제거합니다.

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

단계 **4** 교체 디바이스를 구축합니다.

Cisco Firepower Threat Defense Virtual for VMware 시작 가이드를 참조하십시오.

단계 **5** 교체 디바이스에서 초기 설정을 수행합니다.

VMware 콘솔을 사용하여 관리자로 threat defense virtual 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.

시작 가이드에서 CLI 설정 항목을 참조하십시오. Cisco Firepower Threat Defense Virtual for VMware 시작 가이드

단계 **6** 교체 디바이스가 결함이 있는 디바이스와 동일한 방화벽 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

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

1. CDO에서 threat defense virtual 등록 프로세스를 완료합니다.
2. threat defense virtual 디바이스를 패치합니다.
3. CDO에서 새로 패치한 디바이스 등록을 취소합니다.

단계 **7** 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.

단계 **8** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense virtual 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**

단계 **9** CDO에 로그인하고 디바이스가 연결될 때까지 기다립니다.

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

현재 디바이스가 오래된 것으로 표시됩니다.

단계 **10** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의하십시오.
- HA 동기화를 다시 시작합니다.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense virtual디바이스에서 VPN 인증서를 제거합니다.

단계 **11** 설정을 구축합니다.

반드시 구축해야 합니다. 복구된 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제로 구축합니다.

단계 **12** 디바이스의 데이터 인터페이스를 연결합니다.

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