

Security Cloud Control을 통해 온프레미스 FMC를 클라우드로 마이그레이션(cdFMC)

목차

[문제](#)

[환경](#)

[해결](#)

[원인](#)

[관련 콘텐츠](#)

- [문제](#)
 - [환경](#)
 - [해결](#)
 - [원인](#)
 - [관련 콘텐츠](#)
-

문제

사용자는 SCC(Security Cloud Control) 테넌트의 프로덕션 FMCv300(Firewall Management Center) 가상 어플라이언스를 cdFMC(cloud-delivered FMC)로 마이그레이션하는 데 도움이 필요합니다. 구체적인 우려 사항은 다음과 같습니다.

- 마이그레이션 프로세스의 어떤 부분이 다운타임을 일으킬 수 있는지, 그리고 운영 영향을 최소화할 수 있는 방법을 파악합니다.
- 마이그레이션 워크플로에 대한 단계별 지침을 제공합니다.
- 마이그레이션 완료 후 FMCv300으로 수행할 작업을 결정합니다.
- 고가용성(HA) 컨피그레이션의 여러 FTD(Firewall Threat Defense) 디바이스에 대한 단계별 마이그레이션 접근 방식을 계획합니다.
- 마이그레이션 마법사를 시작하기 전에 온-프레미스 FMC 컨피그레이션을 수동으로 cdFMC로 가져와야 하는지 확인하십시오.

환경

- 소스 FMC: FMCv300 가상 어플라이언스, 버전 7.6.5. 기타 하드웨어(HW) 및 소프트웨어(SW) 플랫폼도 구축할 수 있습니다.
- 대상: cdFMC 테넌트가 프로비저닝되었습니다.
- 관리되는 디바이스는 서로 다른 HW 및 SW 버전의 FTD입니다. 예를 들면 다음과 같습니다.
 - HA 쌍으로 구성된 2x Secure Firewall 3130, FTD 7.6.4.
 - 2x Firepower 2130, FTD 7.4.4, HA 쌍으로 구성
 - Azure에서 1x FTDv, 7.6.4, 독립형 컨피그레이션

해결

마이그레이션 사전 요구 사항 및 버전 검증

환경 버전은 cdFMC로 마이그레이션하기 위한 사전 요구 사항을 충족합니다.

- FMC 7.6.5는 마이그레이션 워크플로에 대한 문서화된 최소 요구 사항을 충족합니다.
- FTD 버전 7.6.4 및 7.4.4는 문서화된 마이그레이션 최소 기준을 충족합니다.
- cdFMC는 환경에서 FTD 릴리스 트레이ンを 지원합니다.

마이그레이션 전 검증 단계

마이그레이션을 시작하기 전에 다음 사전 요구 사항을 검증하십시오.

- FMCv300에서 보류 중인 구축이 없습니다.
- 두 HA는 모두 정상적이고 동기화됩니다.
- FMCv300 백업이 완료되었습니다.
- 사용 가능한 충분한 FMC 디스크 공간(최소 10% 사용 가능)
- FTD 관리 경로에서 작동하는 DNS 확인.
- 필수 클라우드 관리 포트(TCP 443 및 TCP 8305)를 통해 FTD 관리 인터페이스에서 cdFMC로의 아웃바운드 연결이 허용됩니다.

- FMCv300에는 SCC에 대한 아웃바운드 HTTPS 액세스가 있습니다.

컨피그레이션 가져오기 프로세스

마이그레이션 마법사를 실행하기 전에 온프레미스 FMCv300 구성을 수동으로 cdFMC로 가져올 필요는 없습니다. "FTD를 cdFMC로 마이그레이션" 워크플로는 마이그레이션 작업의 일부로 컨피그레이션 가져오기를 처리합니다.

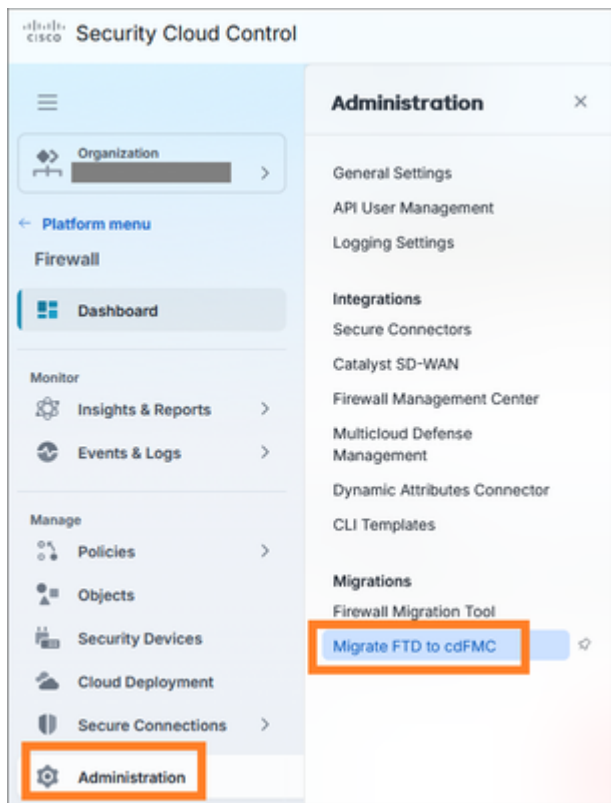
1. SCC가 온프레미스 FMCv300에 연결됩니다.
2. 온프레미스 FMC에서 관련 컨피그레이션을 내보냅니다.
3. 공유 정책/객체를 cdFMC로 가져옵니다.
4. 인터페이스 및 라우팅과 같은 디바이스별 컨피그레이션을 가져옵니다.
5. 선택한 FTD 디바이스를 cdFMC에 등록합니다.
6. 마이그레이션이 완료된 후 14일간의 평가 기간이 시작됩니다.

FMCv300의 항목과 동일한 이름으로 마이그레이션하기 전에 cdFMC에서 정책 또는 개체를 수동으로 만드는 경우 마이그레이션 워크플로에서는 온프레미스 버전을 가져오는 대신 기존 cdFMC 항목을 사용할 수 있으므로 예기치 않은 결과가 발생할 수 있습니다.

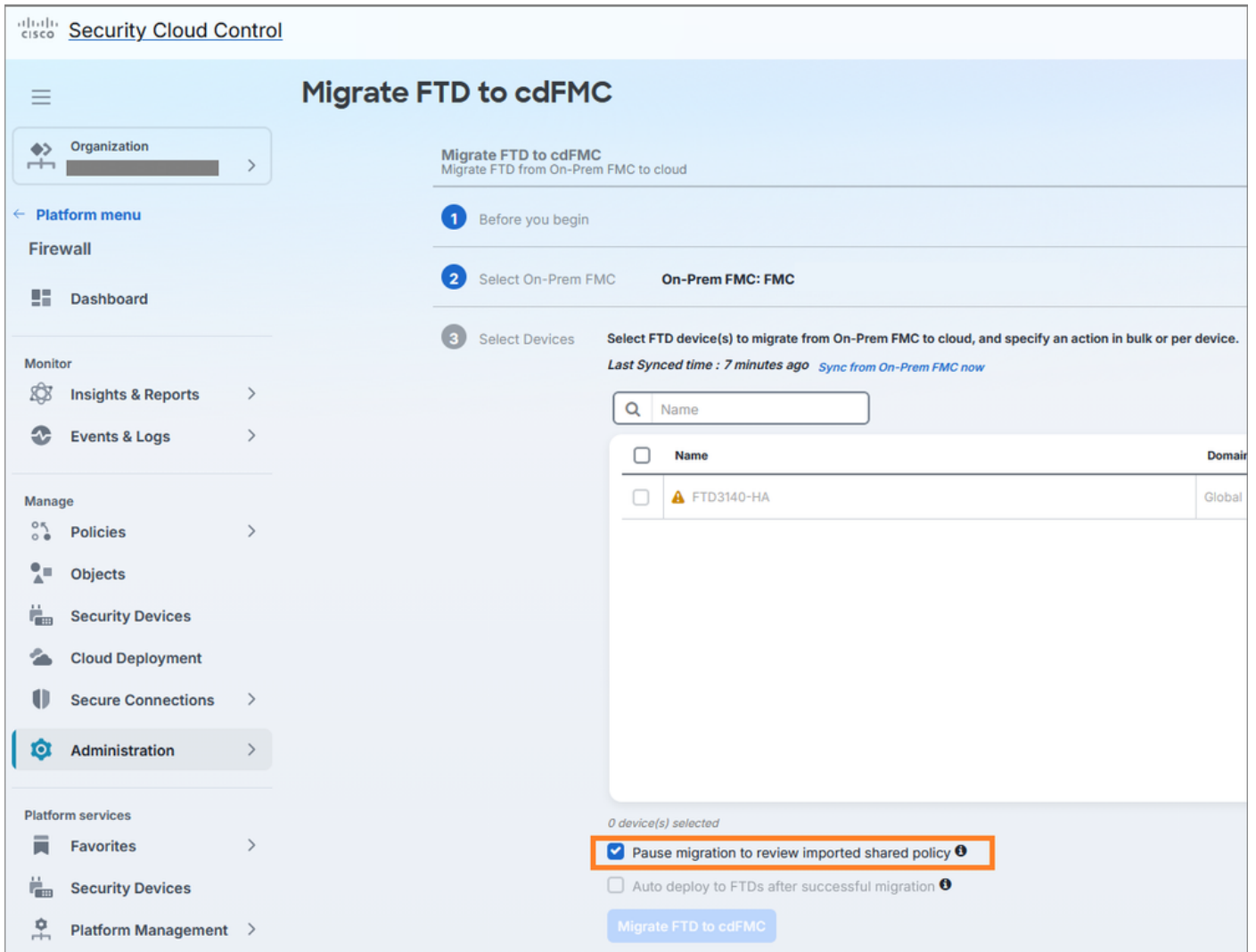
권장 마이그레이션 시퀀스

1단계: 마이그레이션 전 설정

1. SCC 테넌트에 cdFMC를 구축합니다.
2. 현재 FMCv300을 SCC에 온보딩합니다.
3. cdFMC용 Smart Licensing을 확인합니다.
4. Firewall(방화벽) > Administration(관리) > Migrations(마이그레이션) > Migrate FTD to cdFMC(FTD를 cdFMC로 마이그레이션)에서 마이그레이션 워크플로를 시작합니다.



5. 공유 정책 가져오기 후 검토를 위해 일시 중지하려면 이 옵션을 사용합니다.



2단계: 마이그레이션 실행

유지 보수 기간 동안 단계별 접근 방식을 사용하여 디바이스를 마이그레이션합니다.

1. 독립형 FTD로 시작합니다(영향 최소화).
2. 첫 번째 HA 쌍을 마이그레이션합니다.
3. 디바이스 상태 및 기능 검증
4. 두 번째 HA 쌍을 마이그레이션합니다.

3단계: 마이그레이션 후 검증

각 디바이스 또는 HA 쌍 마이그레이션 후:

1. cdFMC에서 디바이스 상태를 확인합니다.
2. 해당되는 경우 HA 상태를 확인합니다.
3. 배포 미리 보기/경고를 검토합니다.
4. cdFMC에서 구축합니다.
5. 트래픽 및 이벤트 가시성 검증

컨피그레이션이 동결되는 3단계 마이그레이션 계획

권장되는 접근 방식에는 3단계로 FTD 마이그레이션을 실행하며 각각 별도의 날짜에 실행되며 단계별로 최소 3일 동안 컷오버 후 모니터링이 이루어집니다. 이러한 접근 방식을 통해 위험을 줄이고 다음을 검증할 시간을 확보할 수 있습니다.

- cdFMC에서 정책 구축.
- 디바이스 상태.
- 두 HA 쌍의 HA 상태.
- 클라우드의 이벤트/분석 가시성.
- 다음 단계로 진행하기 전에 운영 문제가 발생했습니다.

컨피그레이션 동결 구현

다음과 같은 방법으로 마이그레이션/평가 기간 동안 컨피그레이션 종단을 구현합니다.

- 최상의 옵션: 각 단계가 검증되고 커밋될 때까지 FMCv300 및 cdFMC 전체에서 모든 FTD 관련 컨피그레이션 변경 사항을 고정합니다.
- 최소 옵션: 마이그레이션되는 디바이스와 마이그레이션되지 않은 디바이스 모두에서 사용되는 모든 공유 정책/객체를 고정합니다.
- 단계별 마이그레이션 중에는 FMCv300 및 cdFMC에서 동일한 공유 정책/객체를 편집하지 마십시오.
- 평가 기간 동안 큰 변화를 피하십시오.

긴급 변경 프로세스

마이그레이션 중 긴급 변경 사항:

- 해당 디바이스의 현재 권한 있는 관리자에만 변경 사항을 적용합니다.
 - 아직 마이그레이션되지 않은 디바이스: FMCv300.
 - 이미 마이그레이션된 디바이스: cdFMC.
- 변경 사항, 영향을 받는 정책/객체, 타임스탬프 및 디바이스 범위를 문서화합니다.
- 단계가 완료된 후 변경 사항을 조정합니다. 특히 공유 객체 또는 공유 정책에 영향을 주는 경우 더욱 그렇습니다.

평가 기간 관리

14일 평가 기간 동안 중요한 고려 사항:

- 마이그레이션 단계/작업별로 14일 평가 기간을 추적합니다.
- 어떤 단계도 의도치 않게 자동 커밋(auto-commit)에 이르지 않도록 하십시오.
- 3일 모니터링에 성공하면 14일 동안 기다리지 않고 해당 단계를 수동으로 커밋합니다.

FMCv300 서비스 해제 프로세스

디바이스 마이그레이션 직후 FMCv300의 전원을 끄거나 제거하지 마십시오. FMCv300 사용 가능 기간:

- 모든 FTD 디바이스가 성공적으로 마이그레이션됩니다.
- cdFMC 구축에 성공했습니다.
- 클라우드 분석/이벤트가 확인되었습니다.
- 마이그레이션이 커밋됩니다.
- 모든 로그/이벤트 보존 요구 사항이 충족됩니다.
- 최종 FMCv300 백업은 조직 정책에 따라 보존됩니다.

이러한 조건이 충족되면 FMCv300은 표준 가상 머신 사용 중지 프로세스에 따라 활성 사용에서 제거되고 서비스 해제될 수 있습니다.

원인

이는 온프레미스 FMC에서 cdFMC로 계획된 마이그레이션입니다. 이러한 마이그레이션은 클라우드 기반 관리 기능을 활용하고 기존 FMCv300 가상 어플라이언스를 해제해야 하는 필요성에 의해 이루어집니다.

관련 콘텐츠

- [FTD를 cdFMC로 마이그레이션 - Cisco 설명서](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.