FMCv 업그레이드 및 VMware ESXi 7.0에서 ESXi 8.0으로 마이그레이션: 단계별 접근 방식 및 모범 사례

목차

문제

VMware ESXi 7.0에서 FMCv(Firewall Management Center Virtual) 버전 7.3.1을 실행 중인 관리자가 FMC를 지원되는 상위 버전으로 업그레이드한 다음 FMCv 가상 시스템을 새 VMware ESXi 8.0 클러스터로 마이그레이션할 계획입니다. 이러한 우려는 이러한 계획 과정에서 제기되었습니다.

- FMCv를 7.3.1에서 7.4.2로 먼저 업그레이드한 다음 추가 업그레이드를 수행하기 전에 VM을 ESXi 8.0 클러스터로 마이그레이션하는 것이 안전한지 여부.
- 버전 7.3.1 또는 7.4.2를 실행하는 FMCv를 VMware ESXi 8.0 환경으로 마이그레이션할 때 알려진 호환성 문제 또는 제약 조건이 있는지 여부.
- VMware vMotion을 사용하여 새 VM 인스턴스를 생성하지 않고 FMCv 가상 머신을 새 클러스터로 원활하게 동일한 IP 마이그레이션을 수행할 수 있는지 여부.
- 업그레이드 또는 마이그레이션에 실패할 경우 VMware 스냅샷을 백업 및 롤백 메커니즘으로 사용할 수 있는지 여부.
- 버전 7.2.8~7.4.2의 FTD(Firewall Threat Defense) 디바이스를 포함하는 기존 관리되는 디바이스 환경에서 가장 많이 지원되는 FMC 버전은 무엇입니까?
- 동일한 관리 IP 주소 및 호스트 이름을 유지하면서 새 클러스터의 새 FMCv 인스턴스로 이동할 때 IP 주소 충돌을 방지하는 방법.
- 위험과 다운타임을 최소화하는 단계별 업그레이드 및 마이그레이션 계획을 수립하는 것이 올바른 운영 순서입니다.

환경

- 제품: FMCv
- 현재 FMC 소프트웨어 버전: 7.3.1
- 현재 하이퍼바이저 플랫폼: VMware ESXi 7.0
- 대상 하이퍼바이저 플랫폼: VMware ESXi 8.0.3(새 클러스터)
- FMC 구축 유형: 독립형(고가용성 쌍의 일부가 아님)
- 관리되는 디바이스: 버전 7.2.8~7.4.2의 여러 FTD 디바이스

해결

이 환경에 권장되는 접근 방식은 단계별 업그레이드 및 마이그레이션 계획입니다. 이 계획에서는 FMC 소프트웨어 업그레이드, 하이퍼바이저 플랫폼 마이그레이션, 이후의 모든 FMC 버전 업그레이드를 별도의 유지 보수 이벤트로 구분합니다. 이 접근 방식은 각 단계에서 위험을 줄이고 확실한 롤백 지점을 제공합니다. VMware vMotion, 스냅샷, 복제 또는 직접 VM 레벨 마이그레이션을 사용하는 것은 클러스터나 버전 간에 FMCv를 마이그레이션하는 데 지원되는 방법이 아닙니다.

중요: VMware 스냅샷, vMotion 및 클론 작업은 FMCv 마이그레이션에 대해 지원되지 않음

이 계획의 모든 단계를 진행하기 전에 VMware 네이티브 마이그레이션 방법과 관련된 다음과 같은 제약 조건을 이해하는 것이 중요합니다.

- VMware 스냅샷은 FMCv 업그레이드 또는 마이그레이션에 대해 지원되는 백업, 복원 또는 롤백 방법이 아닙니다. FMCv를 VMware 스냅샷으로 되돌리면 데이터베이스 손상, 버전 및 콘텐츠 업데이트 불일치 또는 지원되지 않는 시스템 상태가 발생할 수 있습니다.
- VMware vMotion, 클로닝, 클러스터 간 직접 가상 머신 마이그레이션은 FMCv를 새 하이퍼바이저 플랫폼으로 마이그레이션하는 데 지원되지 않습니다. 이러한 방법은 FMC의 내부 데이터 무결성 메커니즘을 우회합니다.
- FMCv를 새 클러스터 또는 호스트로 마이그레이션하기 위해 지원되는 유일한 방법은 대상 플랫폼에 새 FMCv 인스턴스를 구축하는 것과 결합된 FMC 기본 백업 및 복원 워크플로입니다.

올바른 롤백 전략은 컷오버 후 검증이 실패할 경우 새 FMCv 인스턴스의 전원을 끄고 원래 FMCv를 서비스로 되돌리는 것입니다. 이 용도로 스냅샷 되돌리기를 사용하지 마십시오.

1단계: 업그레이드 전 호환성 검사

FMC 소프트웨어 업그레이드를 시작하기 전에 환경에서 관리되는 모든 FTD 디바이스의 정확한 소프트웨어 버전을 확인합니다.

- FMC 7.4.2는 버전 7.0 이상을 실행하는 FTD 디바이스의 관리를 지원합니다.
- FMC 7.6.6은 버전 7.1 이상을 실행하는 FTD 디바이스의 관리를 지원합니다.
- 환경에 있는 FTD 디바이스에서 버전 7.0을 실행하는 경우 FMC가 버전 7.3.1을 유지하는 동안 해당 디바이스를 버전 7.0 이상으로 업그레이드해야 FMC 자체를 업그레이드할 수 있습니다.
- 문서화된 환경(FTD 범위: 7.2.8 - 7.4.2), 모든 관리되는 디바이스는 FMC 7.4.2 및 FMC 7.6.6의 호환성 범위에 있습니다. 이 경우에는 FTD 사전 업그레이드가 필요하지 않습니다.

계속하기 전에 다음 사항도 확인하십시오.

- FMC는 독립형이며 고가용성(HA) 쌍의 일부가 아닙니다.
- 새 클러스터에 정확한 VMware ESXi 8.0이 구축됩니다(이 환경에서 ESXi 8.0.3으로 확인).
- FMCv 리소스 프로필(vCPU, 메모리, 디스크)은 대상 FMC 릴리스의 요구 사항을 충족합니다. 4개의 vCPU, 32GB RAM 및 250GB 디스크의 현재 사양은 특히 FMC 7.6.6으로 업그레이드하기 전에 현재 구축 지침과 비교하여 검토해야 합니다.
- 마이그레이션 후에도 FMC 관리 IP 주소와 호스트 이름이 동일하게 유지되는지 여부(모든 관리되는 FTD 디바이스에서 관리자 주소 업데이트가 필요하지 않도록 하는 것이 좋습니다.)

2단계: 현재 ESXi 7.0 클러스터에서 기존 FMCv를 7.3.1에서 7.4.2로 업그레이드

이 단계에서는 기존 ESXi 7.0 인프라에 FMCv 소프트웨어를 유지하면서 버전 7.4.2로 업그레이드합니다. FMCv 7.4.2는 3단계에서 플랫폼을 마이그레이션하기 전에 필요한 VMware ESXi 8.0에 대한 명시적 지원을 추가합니다.

1단계: 업그레이드를 시작하기 전에 보류 중인 정책 배포, 활성 백업 작업 또는 백그라운드 작업이 현재 FMC에서 실행되고 있지 않은지 확인합니다.

2단계: FMC 기본 제공 백업 유틸리티를 사용하여 전체 기본 FMC 백업을 수행합니다. FMCv 가상 머신 외부의 안전한 원격 위치에 백업을 저장합니다. 계속하기 전에 백업이 성공적으로 완료되었는지 확인합니다.

3단계: FMC 7.4 업그레이드 계획 가이드에 설명된 대로 모든 업그레이드 준비 상태 점검을 완료합니다. 업그레이드를 시작하기 전에 플래그가 지정된 문제를 모두 해결합니다.

4단계: 기존 FMCv를 버전 7.3.1에서 버전 7.4.2로 업그레이드합니다. 지원되는 업그레이드 전환 경로가 사용됩니다. 7.3→7.4.

5단계: 업그레이드가 완료되면 업그레이드 후 검증을 수행합니다.

- 모든 관리되는 FTD 디바이스가 FMC에 다시 연결되었는지 확인합니다.
- 이벤트 수집이 활성 상태이고 FMC에 이벤트가 표시되는지 확인합니다.
- 라이센스 상태가 올바른지 확인합니다.
- 관리되는 디바이스에 대한 테스트 정책 구축을 실행하고 성공 여부를 확인합니다.

업그레이드된 FMCv 7.4.2에서 모든 업그레이드 후 검증 단계가 성공적으로 통과될 때까지 3단계로 진행하지 마십시오.

3단계: 네이티브 백업 및 복원을 사용하여 VMware ESXi 8.0.3 클러스터로 FMCv 마이그레이션

이 단계에서는 FMCv를 기존 ESXi 7.0 클러스터에서 새 ESXi 8.0.3 클러스터로 마이그레이션합니다. 이렇게 하려면 대상 클러스터에 새 FMCv 인스턴스를 구축하고 기본 FMC 백업을 복원합니다. 관리되는 모든 FTD 디바이스에서 관리자 주소를 변경하지 않아도 되도록 동일한 관리 IP 주소 및 호스트 이름이 유지됩니다.

1단계: 버전 7.4.2에서 FMCv가 안정적인 것으로 확인되면 새로운 네이티브 FMC 백업을 생성합니다. 안전한 원격 위치에 저장하십시오. 계속하기 전에 백업이 완료되고 유효한지 확인하십시오.

2단계: ESXi 8.0.3 클러스터에 새 FMCv 인스턴스를 구축합니다. 이 새 인스턴스의 소프트웨어 버전 및 빌드는 백업(FMCv 7.4.2)이 수행된 FMCv 버전(패치 및 핫픽스 포함)과 정확히 일치해야 합니다. 새 인스턴스가 동급 이상의 리소스(vCPU, 메모리, 디스크)로 구성되어 있고 네트워크 컨피그레이션이 준비되었지만 현재 프로덕션 관리 IP 주소가 새 인스턴스에 아직 할당되지 않았는지 확인합니다.

3단계: 네이티브 FMC 백업을 ESXi 8.0.3의 새 FMCv 인스턴스로 복원합니다.

4단계: 운영 관리 IP 주소 및 호스트 이름을 사용하여 새 FMCv를 온라인 상태로 전환하기 전에 네트워크에서 원래 FMCv의 전원을 완전히 끄거나 연결을 끊습니다. 이는 중복 IP 조건을 방지하고 두 FMC 인스턴스가 동일한 관리되는 FTD 디바이스와 동시에 통신하려고 시도하는 것을 방지하기 위한 필수 단계입니다.

원래 FMCv의 전원이 꺼지고 새 FMCv가 온라인 상태가 되기 전에 관리되는 FTD 디바이스에서 다음 동작이 예상됩니다.

- 트래픽 전달: FTD 디바이스는 FMC와 독립적으로 데이터 플레인을 운영하고, 여기에서 언급한 경우를 제외하고 계속해서 트래픽을 원활하게 전달하고 마지막으로 성공적으로 구축된 액세스 제어 정책을 적용합니다.
- 관리 및 가시성 변경: 정책 구축, 컨피그레이션 조정, FMC 상태 알림, 디바이스 관리 가시성을 완전히 사용할 수 없습니다.
- 이벤트 버퍼링 및 잠재적 손실: FMC에서 실시간 이벤트 가시성이 일시 중지됩니다. FTD는 임시 통합 파일에 보안 및 연결 이벤트를 로컬로 로깅하려고 시도하는 반면, 이러한 파일은 엄격한 스토리지 제한을 가지며 순환 덮어쓰기 기반으로 작동합니다. 대용량 연결 로그는 확장 마이그레이션 기간 중에 덮어쓰거나 손실될 수 있습니다. 로컬 버퍼에 남아 있는 이벤트는 온라인 상태가 되면 새 FMC로 스트리밍됩니다.
- 악성코드(AMP) 규칙: FMC는 이러한 평판 쿼리를 AMP 클라우드에 프록시하므로 캐시되지 않은 파일에 대한 실시간 클라우드 조회 요청을 일시적으로 사용할 수 없습니다. FTD는 로컬 온박스 처리 캐시에 이미 저장된 파일에 대해서만 차단 또는 허용 규칙을 계속 적용합니다. 캐시되지 않은 파일은 클라우드 분석을 건너뛰고 정책의 Fail-Safe 설정을 사용합니다(일반적으로 트래픽 중단을 방지하기 위해 Fail Open). Threat Grid에 대한 샌드박싱 제출 및 회귀적 알림은 새 FMC가 작동할 때까지 일시 중지됩니다.
- ID 기반 규칙: 이미 로그인되어 IP 주소에 매핑된 사용자는 FTD가 활성 매핑을 로컬 메모리에 유지하기 때문에 중단 없이 사용할 수 있습니다. 그러나 FMC는 ID 소스(예: Cisco ISE 또는 Active Directory 에이전트)에 대한 브로커 역할을 하기 때문에 이 기간 동안 새 사용자 로그인 또는 IP 변경 사항을 FTD에서 확인할 수 없습니다. 이러한 알 수 없는 세션은 정책의 기본 또는 게스트 규칙으로 돌아갑니다.
- URL 필터링: FMC가 알 수 없는 URL 요청을 Cisco Talos 클라우드로 프록시하기 때문에 완전히 알 수 없는 웹 사이트에 대한 실시간 클라우드 조회를 일시적으로 사용할 수 없습니다. FTD는 푸시된 로컬 데이터 집합 또는 활성 로컬 메모리 캐시 내에 이미 있는 웹 사이트에 대해서만 정책을 완전히 필터링하고 적용합니다. 캐시되지 않은 알 수 없는 URL에 도달하는 웹 트래픽은 클라우드 분류를 우회하고 분류되지 않은 트래픽에 대한 정책의 대체 설정을 일치시킵니다(일반적으로 허용됨). 새 FMC가 온라인 상태가 될 때까지 URL 데이터베이스 패키지 업데이트가 일시 중지됩니다.

5단계: ESXi 8.0.3에서 복원된 FMCv에 운영 관리 IP 주소 및 호스트 이름을 지정하고 온라인으로 전환합니다. 동일한 IP 주소 및 호스트 이름이 사용되므로, 관리되는 FTD 디바이스는 개별 FTD 디바이스에서 관리자-주소를 변경하지 않고도 FMC에 자동으로 다시 연결할 수 있습니다.

6단계: 마이그레이션 후 검증 수행:

- 모든 관리되는 FTD 디바이스가 새 FMCv 인스턴스에 다시 연결되었는지 확인합니다.
- 라이선스 상태를 확인하고 모든 라이선스가 올바르게 적용되었는지 확인합니다.
- 이벤트 흐름 및 외부 통합이 올바르게 작동하는지 확인합니다.
- 관리되는 디바이스에 제어된 정책 구축을 실행하고 성공 여부를 확인합니다.

이 단계에서 검증이 실패하면 새 FMCv 인스턴스를 끄고 ESXi 7.0의 원래 FMCv를 서비스로 복원한 다음 마이그레이션을 다시 시도하기 전에 문제를 해결합니다. VMware 스냅샷 되돌리기를 롤백 메커니즘으로 사용하지 마십시오.

4단계: FMCv를 7.4.2에서 7.6.6으로 업그레이드(마이그레이션이 안정적인 것으로 확인된 후)

ESXi 8.0.3으로의 FMCv 마이그레이션이 완전히 검증되고 안정적임을 확인한 후에는 FMC 7.6.6으로의 업그레이드를 고려할 수 있습니다. 하이퍼바이저 플랫폼 마이그레이션(3단계)과 이 추가 FMC 버전 업그레이드는 단일 유지 관리 이벤트로 결합하지 않는 것이 좋습니다. 마이그레이션을 먼저 완료하면 계속하기 전에 위험도가 낮은 클린 체크포인트가 제공됩니다.

7.6.6으로 업그레이드하기 전에 다음 전제 조건을 확인하십시오.

- 환경의 모든 관리되는 FTD 디바이스는 버전 7.1 이상을 실행하고 있습니다. FMC 7.6.6은 FTD 디바이스 < 버전 7.1의 관리를 지원하지 않습니다. 문서화된 환경(FTD 범위: 7.2.8 ~ 7.4.2), 모든 디바이스가 이 요구 사항을 충족합니다.
- FMCv 리소스 프로파일(4개의 vCPU, 32GB RAM, 250GB 디스크)이 이 환경의 전체 관리되는 디바이스 수 및 이벤트 보존 요구 사항에 대한 FMC 7.6.6 구축 지침에 따라 검증되었습니다.
- 지원되는 업그레이드 전환 경로가 확인되었습니다. 7.4→7.6.
- FMC는 독립형(고가용성 쌍의 일부가 아님)으로 확인됩니다.

1단계: ESXi 8.0.3의 안정적인 FMCv 7.4.2 인스턴스에서 새로운 네이티브 FMC 백업을 만들고 확인합니다. 안전한 원격 위치에 저장합니다.

2단계: FMCv를 버전 7.4.2에서 버전 7.6.6으로 업그레이드합니다.

3단계: 최종 업그레이드 후 검증 수행:

- 모든 관리되는 FTD 디바이스가 FMC에 다시 연결되었는지 확인합니다.
- 이벤트 처리 및 이벤트 수집이 올바르게 작동하는지 확인합니다.
- 라이센스 상태가 올바른지 확인합니다.
- 제어된 정책 구축을 실행하여 정책 애플리케이션이 성공적인지 확인합니다.

업그레이드 경로 및 전환 순서 요약

이 표에는 모든 준비된 계획, 지원되는 업그레이드 전환 및 각 단계의 주요 작업이 요약되어 있습니다.

단계	작업	FMC 버전	하이퍼바이저	지원되는 전환
1단계	업그레이드 전 호환성 검사; ftd 버전, FMC HA 상태 및 리소스 프로필 확인	7.3.1(현재)	ESXi 7.0	해당 사항 없음 — 준비만
2단계	FMCv 소프트웨어 업그레이드; 네이티브 백업 수행 관리되는 디바이스 및 정책 구축 검증	7.3.1→7.4.2	ESXi 7.0	7.3 → 7.4(지원됨)
3단계	ESXi 8.0.3에 새 FMCv 구축 네이티브 백업 복원; 동일한 IP/호스트 이름을 사용하여 컷오버합니다. 유효성 검사	7.4.2(버전 변경 없음)	ESXi 7.0 → ESXi 8.0.3	기본 백업/복원 - 지원되는 방법
4단계	마이그레이션 후 안정적: FMCv 업그레이드 디바이스 연결, 라이센싱, 이벤트, 정책 검증	7.4.2→7.6.6	ESXi 8.0.3	7.4 → 7.6(지원됨)

주요 고려 사항

- 업그레이드 경로 규정 준수: 전체 업그레이드 시퀀스(7.3.1 → 7.4.2 → 7.6.6)는 지원되는 FMC 업그레이드 전환 경로(7.3 → 7.4 및 7.4 → 7.6)를 사용합니다. 중간 버전을 건너뛰거나 단계를 단일 이벤트로 결합하는 것은 권장되지 않습니다.

- FMC-FTD 호환성: FMC 7.6.6은 버전 7.2.8~7.4.2를 실행하는 FTD 디바이스와 완전한 관리 호환성을 유지합니다. FMC 7.6에서는 모든 관리되는 FTD 디바이스가 버전 7.1 이상이어야 합니다.
- 동일한 IP 주소 전환: 교체 FMCv가 프로덕션 관리 IP 주소로 온라인 상태가 되기 전에 원래 FMCv의 전원을 완전히 끄거나 네트워크에서 연결을 끊어야 합니다. 이렇게 하면 중복 IP 조건을 방지할 수 있으며, 두 관리 센터에서 동시에 동일한 FTD 디바이스와의 통신을 시도하는 것을 방지할 수 있습니다. 복원된 FMCv가 동일한 IP 주소 및 호스트 이름으로 반환되면, 관리되는 FTD 디바이스는 관리자 주소 변경 없이 다시 연결할 수 있습니다.
- 7.6.6 이전의 리소스 검증: FMCv 리소스 프로파일(4개의 vCPU, 32GB RAM, 250GB 디스크)을 현재 구축 지침과 비교하여 검토해야 FMC 7.6.6으로 업그레이드할 수 있습니다. 이는 환경에 대한 총 관리 디바이스 수 및 이벤트 보존 요구 사항을 고려해야 합니다.
- 기본 백업 확인: 네이티브 FMC 백업을 수행하는 각 단계에서 백업을 완료하고 유효한 것으로 확인한 다음 진행해야 합니다. 백업은 FMCv 가상 머신 외부의 안전한 원격 위치에 저장해야 합니다.
- 마이그레이션 및 업그레이드 통합 안 함: 플랫폼 마이그레이션(3단계) 및 후속 FMC 버전을 7.6.6으로 업그레이드(4단계)는 별도의 유지 보수 이벤트로 수행해야 합니다. 따라서 ESXi 8.0.3의 FMCv 7.4.2에 안전한 체크포인트가 존재하므로 추가 변경이 이루어집니다.

원인

이는 소프트웨어 결함 또는 잘못된 컨피그레이션으로 인한 고장 수리 문제가 아닙니다. 이 지침이 필요한 근본적인 원인은 VMware의 Cisco FMCv와 관련된 버전 호환성 요구 사항 및 플랫폼 마이그레이션 제약 조건이 결합되어 있기 때문입니다.

- FTD 7.4.2와의 FMC 버전 호환성: 이전 FMC 버전에서는 FMC 자체보다 상위 버전의 FTD 디바이스를 관리할 수 없으므로, 환경에서 버전 7.4.2를 실행하는 관리되는 FTD 디바이스가 있으면 FMC를 최소 버전 7.4.2로 업그레이드해야 합니다.
- VMware ESXi 8.0에 대한 FMCv 지원: FMCv 7.3.1은 VMware ESXi 8.0을 하이퍼바이저 플랫폼으로 지원하지 않습니다. ESXi 8.0.x에서 FMCv를 구축하거나 운영하려면 먼저 버전 7.4.2 이상으로 업그레이드해야 합니다. 먼저 FMC 소프트웨어를 업그레이드하지 않고 FMCv 7.3.1 VM을 ESXi 8.0으로 직접 마이그레이션하려고 하면 호환성 위험이 발생합니다.
- 지원되지 않는 VM 마이그레이션 방법: VMware vMotion, 스냅샷, 복제 및 직접 VM 마이그레이션은 클러스터 또는 하이퍼바이저 버전 간에 FMCv를 마이그레이션하는 데 지원되지 않습니다. 이러한 메서드는 데이터베이스 손상, 버전 불일치 또는 지원되지 않는 시스템 상태를 초래할 수 있습니다. 지원되는 유일한 마이그레이션 경로는 FMC 네이티브 백업 및 복원 워크플로와 대상 플랫폼의 새로운 FMCv 구축입니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center 업그레이드 가이드, 버전 7.4 — 업그레이드 계획 및 지원되는 경로
- Cisco Secure Firewall Management Center 업그레이드 가이드, 버전 7.6 — 업그레이드 계획 및 지원되는 경로
- Cisco Secure Firewall Management Center 호환성 가이드(FMC 및 FTD 호환성 매트릭스)
- Cisco Secure Firewall Management Center 릴리스별 새로운 기능 - 버전 7.4.2
- Cisco Firepower Management Center 업그레이드 가이드 — 업그레이드 계획
- 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.