SD-WAN cEdge 라우터에서 Secure Factory Reset 수행

목차

소개

이 문서에서는 Cisco IOS® XE를 실행하는 Cisco Catalyst SD-WAN Edge Router의 공장 초기화 절차에 대해 설명합니다.

배경

공장 재설정은 디바이스를 원래 제조 상태로 되돌리며 일반적으로 서비스 해제, 재구축 또는 보안 교정 워크플로의 일부로 필요합니다.

⚠

주의: 이 문서에서는 NIST SP 800-88 Rev. 1에 맞춰 데이터 정화를 수행하는 `factory-reset all secure` 옵션을 독점적으로 권장합니다. 이 방법을 사용하면 스토리지 미디어의 데이터를 복구할 수 없게 되며 중요한 데이터가 영구적으로 제거되었음을 최고 수준으로 확인할 수 있습니다.

적용 가능성

factory-`reset all secure` 명령은 Cisco IOS XE를 실행하는 다음 플랫폼에서 지원됩니다.

- Cisco Catalyst 8200 Series Edge Platform
- Cisco Catalyst 8300 Series Edge Platform
- Cisco Catalyst 8500 Series Edge Platform
- Cisco ASR 1000 Series Aggregation Services 라우터
- Cisco ISR 4000 Series Integrated Services Router
- Cisco ISR 1000 Series Integrated Services Router

참고: `all secure` 옵션은 독립형 디바이스에서만 사용할 수 있습니다. Factory-reset 을 선택하여 플랫폼과 Cisco IOS XE 버전이 `secure` 키워드를 지원하는지 확인합니다. 계속 진행하기 전에 특권 EXEC 모드에서

사전 요구 사항

Secure Factory 재설정을 수행하기 전에 다음 전제 조건을 충족해야 합니다.

- 백업 구성: 재설정하기 전에 SD-WAN 관리자(vManage)에서 모든 디바이스 컨피그레이션, 템플릿 및 정책을 내보내고 안전하게 저장합니다.
- 백업 소프트웨어 이미지: 재설정을 수행하기 전에 bootflash에 Cisco IOS XE 소프트웨어 이미지의 복사본이 로드되었는지 확인합니다. 보안 옵션은 대부분의 플랫폼에서 부트 이미지를 플래시로 유지하지만, 특정 플랫폼은 보안 지우기의 일부로 bootflash를 완전히 제거합니다. 플랫폼 동작에 관계없이 복구를 보장하려면 항상 USB 드라이브 또는 액세스 가능한 TFTP 서버에서 Cisco IOS XE 이미지를 사용할 수 있어야 합니다.
- 무정전 전원: 재설정 프로세스 전반에 걸쳐 디바이스에 무중단 전원 공급 장치가 있는지 확인합니다. 소독 중 전력 손실은 장치를 복구 할 수 없게 만들 수 있습니다.
- 모든 ISSU 절차를 완료합니다. ISSU(In-Service Software Upgrade) 작업이 보류 중이거나 진행 중인 경우 공장 재설정을 시작하기 전에 완료하십시오.
- 릴리스 HSEC 라이센스: 공장 재설정을 수행하기 전에 디바이스에서 HSEC 라이센스를 해제해야 합니다. Cisco Edge 라우터에서 HSECK9 라이센스 구성 섹션의 "HSECK9 라이센스 반환"에 설명된 대로 HSECK9 라이센스를 반환합니다.

- SD-WAN 패브릭에서 제거: 재설정을 수행하기 전에 vManage에서 디바이스 인증서를 무효화하고 컨트롤러 오버레이에서 디바이스를 제거합니다.
- 콘솔 액세스: 디바이스에 대한 물리적 콘솔 액세스 권한이 있는지 확인합니다. 재설정 후 디바이스가 ROMMON 모드로 전환되고 VTY 세션을 사용할 수 없습니다.

팁: Cisco IOS XE 이미지가 bootflash에 로드되었는지, 그리고 공장 초기화를 실행하기 전에 USB 또는 TFTP에서 복구 복사본을 사용할 수 있는지 확인합니다. `secure` 옵션은 대부분의 플랫폼에서 부트 이미지를 유지하지만, 일부 플랫폼은 프로세스 중에 bootflash를 완전히 제거합니다.

지워지는 내용

factory-`reset all secure` 명령은 디바이스에서 이 데이터를 영구적으로 제거합니다.

카테고리	지워진 데이터
소프트웨어	모든 Cisco IOS XE 소프트웨어 이미지(현재 부트 이미지는 대부분의 플랫폼에서 플래시에 유지 그러나 특정 플랫폼에서 bootflash는 완전히 삭제됨)
설정	시작 컨피그레이션, 실행 중인 컨피그레이션
로그 및 진단	충돌 정보, 시스템 로그, OBFL(온보드 장애 로깅)
보안 자료	FIPS 관련 키 및 자격 증명, 사용자 구성 PKI 키 및 인증서
스토리지	이동식 스토리지(SATA, SSD, USB)의 모든 사용자 데이터
라이센싱	모든 디바이스 라이센스(재등록 필요)
ROMMON	사용자 추가 ROMMON 환경 변수

참고: 이러한 항목은 보안 공장 재설정 후 보존됩니다.

- SUDI(Secure Unique Device Identifier) 인증서 및 연결된 PKI 키
- 컨피그레이션 레지스터 값
- 현재 부트 이미지(대부분의 플랫폼에서 플래시에 유지) 특정 플랫폼에서 bootflash는 완전히 삭제됨 - 항상 USB/TFTP 복구를 준비함)

절차: Secure Factory 재설정

경고: 이 절차는 되돌릴 수 없습니다. 일단 시작되면 이전 테이블에 나열된 모든 데이터가 영구적으로 삭제됩니다. 계속하기 전에 모든 백업이 확인되었는지 확인합니다.

1단계: 콘솔을 통해 장치 액세스

물리적 콘솔 연결을 통해 디바이스에 연결합니다. 재설정 프로세스 중에 SSH/VTY 액세스가 손실됩니다.

2단계: 특별 권한 EXEC 모드 시작

```
Device> enable
Device#
```

3단계: Secure Factory 재설정 실행

다음 명령을 실행하여 보안 공장 재설정을 시작합니다.

```
Device# factory-reset all secure
```

확인 메시지가 표시됩니다.

```
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
```

⚠ 확인: 확인 프롬프트에서 다음을 확인하는 마지막 시간을 확인합니다.

- 모든 컨피그레이션이 백업됨
- Cisco IOS XE 복구 이미지는 USB 또는 TFTP에서 사용할 수 있습니다
- 디바이스가 SD-WAN 오버레이에서 제거되었습니다.

`y`를 입력하거나 Enter를 눌러 확인하고 진행합니다.

4단계: 삭제 작업이 완료될 때까지 대기

장치는 모든 저장 매체에서 데이터 삭제를 수행합니다. 이 프로세스는 스토리지 용량에 따라 시간이 오래 걸릴 수 있습니다. 이 작업 중에는 전원을 끄지 마십시오.

완료되면 디바이스가 자동으로 다시 로드되고 ROMMON 모드로 들어갑니다.

5단계: ROMMON 환경 변수 복원

재설정 후 MAC_ADDRESS 및 SERIAL_NUMBER를 포함한 환경 변수를 지울 수 있습니다. ROMMON 재설정을 수행하여 복원합니다.

```
rommon 1> reset
```

참고: BAUD 속도 환경 변수는 공장 초기화 후 기본값(9600)으로 돌아갑니다. 콘솔 세션이 다른 전송 속도로 구성된 경우 터미널 에뮬레이터 설정을 9600 baud로 조정하여 콘솔 액세스를 다시 가져올 수 있습니다.

6단계: Cisco IOS XE 소프트웨어 이미지 부팅

대부분의 플랫폼에서 secure 옵션은 부트 이미지를 플래시에 유지합니다. dir bootflash를 사용하여 존재 확인: ROMMON에서 가져옵니다. 이미지를 사용할 수 있는 경우 직접 부팅합니다.

```
rommon 2> boot bootflash:<image-filename>.bin
```

> 플랫폼별 동작: 특정 하드웨어 플랫폼에서 보안 삭제 프로세스는 부팅 이미지를 포함하여 bootflash를 완전히 삭제합니다. 이러한 경우 USB 또는 TFTP를 통해 복구합니다.
>
> 옵션 A — USB 복구:
>
> ```
> rommon 2> boot usbflash0:<image-filename>.bin
> ```
>
> 옵션 B — TFTP 복구:
>
> 필수 ROMMON 환경 변수를 설정한 다음 전송을 시작합니다.
>
> ```
> rommon 2> IP_ADDRESS=
> ```

```
rommon 3> IP_SUBNET_MASK=

rommon 4> DEFAULT_GATEWAY=

rommon 5> TFTP_SERVER=

rommon 6> TFTP_FILE=

     .bin
rommon 7> tftpboot
```

관리 인터페이스 또는 직접 연결된 네트워크 세그먼트를 통해 TFTP 서버에 연결할 수 있는지 확인합니다. ROMMON은 라우팅 프로토콜을 지원하지 않으므로 구성된 기본 게이트웨이를 통해 TFTP 서버에 연결할 수 있어야 합니다.

이 동작을 고려하여 공장 초기화를 시작하기 전에 항상 USB 또는 액세스 가능한 TFTP 서버에 복구 이미지를 준비해야 합니다.

재설정 후: SD-WAN 패브릭에 다시 온보딩

깨끗한 Cisco IOS XE 이미지로 디바이스를 복원한 후 표준 SD-WAN 온보딩 절차를 사용하여 디바이스를 패브릭으로 다시 가져옵니다.

1. 부트스트랩 구성: 초기 부트스트랩 컨피그레이션(시스템 IP, 사이트 ID, 조직 이름, vBond 주소)을 적용합니다. 절차에 대해서는 CLI를 사용하여 부트스트랩 파일 생성을 참조하십시오.
2. 인증서 설치: 인증 기관(Symantec/DigiCert, Cisco PKI 또는 Enterprise CA)의 필요에 따라 디바이스 인증서 및 루트 CA 체인을 설치합니다.
3. 제어 연결: DTLS/TLS 제어 연결이 vManage, vSmart 및 vBond에 설정되었는지 확인합니다.
4. 템플릿 푸시: vManage에서 적절한 디바이스 템플릿 또는 컨피그레이션 그룹을 디바이스에 연결합니다.
5. 검증: BFD 세션, OMP 경로 및 데이터 플레인 터널이 작동하는지 확인합니다.

참고: 다시 온보딩 후 암호화 처리량을 복원하려면 CLI를 통해 HSEC(High Security) 라이센스를 수동으로 다시 적용해야 합니다. Cisco Catalyst SD-WAN에서 HSEC 라이센스 관리에 설명된 대로, vManage(SD-WAN Manager)는 디바이스에 HSEC 라이센스 재설치를 지원하지 않습니다. 라이센스를 활성화하려면 물리적 라우터에서 디바이스를 다시 로드해야 합니다. 수동 CLI 절차는 Cisco Edge Router에 HSECK9 라이센스 구성을 참조하십시오.

문제 해결

재설정 후 콘솔이 응답하지 않음

공장 재설정이 완료된 후 콘솔이 응답하지 않는 것으로 표시되면 전송 속도가 기본값(9600)으로 되돌려진 것입니다. 터미널 에뮬레이터를 9600 보드로 조정하고 다시 연결합니다.

디바이스가 ROMMON을 입력하지 않음

재설정이 완료된 후 디바이스에서 ROMMON을 입력하지 않으면 컨피그레이션 레지스터가 올바르게 설정되었는지 확인합니다. 대부분의 경우 부팅 가능한 이미지가 없는 경우 전원 사이클이 디바이스를 ROMMON으로 강제 전환합니다.

ROMMON에 환경 변수가 없습니다.

재설정 후 `MAC_ADDRESS` 또는 `SERIAL_NUMBER` 변수가 없는 경우 ROMMON에서 `reset` 명령을 실행하여 하드웨어 스토리지에서 공장 기본 환경 변수를 복원합니다.

자주 묻는 질문(FAQ)

Q: "secure" 옵션이 표준 "all" 또는 "3-pass" 옵션보다 권장되는 이유는 무엇입니까?

A : factory-`reset all secure` 옵션은 NIST SP 800-88 Rev. 1에 맞춰 제공되는 가장 철저한 데이터 삭제 작업을 수행합니다. 데이터를 복구할 수 없게 만들고 현재 부팅 이미지를 플래시에 유지하므로 복구가 간단합니다. 이와 달리 `3-pass` 옵션은 3회 덮어쓰기 패턴(0, 1, 임의)을 수행하므로 시간이 약 3배 더 걸리며 부팅 이미지도 지워지므로 USB 또는 TFTP에서 전체 이미지를 다시 로드해야 합니다. 보안 옵션은 복구를 위한 운영 오버헤드가 가장 적은 위생을 제공하므로 권장됩니다.

Q: Secure Factory Reset은 시간이 얼마나 걸립니까?

A : 기간은 디바이스의 총 스토리지 용량에 따라 달라집니다. 표준 플래시 스토리지(8-32GB)가 있는 디바이스의 경우 일반적으로 프로세스는 15-45분 이내에 완료됩니다. 더 큰 SSD 또는 SATA 스토리지가 있는 장치는 더 오래 걸릴 수 있습니다. 중요: 이 프로세스 중에 전원을 차단하지 마십시오. 재설정 + 이미지 다시 로드 및 재온보딩 시간을 고려하는 유지 관리 기간을 계획합니다.

Q: 재설정 후에도 디바이스의 ID(일련 번호, SUDI)가 유지됩니까?

A : 예. SUDI(Secure Unique Device Identifier) 인증서 및 관련 PKI 키는 하드웨어 보호 스토리지(TAm/ACT2 칩)에 저장되며 공장 재설정에 의해 지워지지 않습니다. 장치 일련 번호는 하드웨어에서도 유지됩니다. 즉, 재설정 후 디바이스를 원래 ID를 사용하여 SD-WAN 패브릭에 재온보딩할 수 있습니다.

Q: 재설정을 수행하기 전에 SD-WAN Manager에서 디바이스를 제거해야 합니까?

A : 예. 공장 재설정을 수행하기 전에 디바이스 인증서를 무효화하고 SD-WAN 오버레이에서 디바이스를 제거하는 것이 좋습니다. 이렇게 하면 컨트롤러 인프라에서 클린 제거가 보장되고, vManage 디바이스 인벤토리에 오래된 항목이 없으며, 분리된 제어 연결 또는 터널 상태가 방지됩니다. vManage에서: Configuration(컨피그레이션) > Certificates(인증서) > device(디바이스) > Invalidate(무효화)를 선택한 다음 Send to Controllers(컨트롤러로 전송)로 이동합니다. 그런 다음 디바이스 목록에서 디바이스를 삭제합니다.

Q: 공장 초기화 후 HSEC 라이센스는 어떻게 됩니까?

A : 공장 초기화 과정에서 HSEC(High Security) 라이센스가 제거됩니다. 이 기능이 없으면 디바이스는 제한된 암호화 처리량으로 작동합니다. HSEC 라이센스는 공장 초기화 전에 릴리스되어야 나중에 다시 사용할 수 있습니다.

1. 재설정 전: 라이센스 스마트 권한 부여를 통해 라이센스를 릴리스하고 로컬로 온라인으로 되돌리고 Smart License Central에서 제품 인스턴스를 제거합니다.
2. 재온보딩 후: CLI를 통해 수동으로 HSEC 라이센스를 다시 적용합니다. Cisco Catalyst SD-WAN에서 HSEC 라이센스 관리에 설명된 대로, vManage(SD-WAN Manager)는 HSEC 라이센스 재설치를 지원하지 않습니다.
3. Reload: 라이센스를 활성화하려면 물리적 라우터에서 다시 로드해야 합니다.
4. `show license summary` 및 `show license authorization`을 통해 확인합니다.

전체 절차는 Cisco Edge Router에 HSECK9 라이센스 구성 및 Cisco Catalyst SD-WAN에서 HSEC 라이센스 관리를 참조하십시오.

Q: SSH/VTY를 통해 원격으로 출고 시 보안 재설정을 수행할 수 있습니까?

A : 이 명령은 SSH/VTY 세션을 통해 기술적으로 실행할 수 있지만 권장하지 않습니다. 디바이스가 즉시 삭제되기 시작하고 원격 세션이 종료됩니다. 재설정 후 디바이스는 ROMMON 모드로 들어갑니다. 이 모드에서는 IP 연결이 제공되지 않으며 VTY 액세스가 불가능하고 이미지 복구를 위해 콘솔 액세스가 필요합니다. 공장 재설정을 시작하기 전에 항상 물리적 콘솔 액세스를 사용할 수 있는지 확인합니다.

Q: 보안 공장 재설정이 보안 교정 시나리오에 적합합니까?

A : 예. 안전한 공장 재설정은 보안 침해가 의심되는 경우 디바이스를 정상 작동이 확인된 상태로 되돌려야 하는 경우 권장되는 방법입니다. 이를 통해 공격자가 심어놓은 모든 키, 백도어 또는 지속성 메커니즘이 영구적으로 제거되고, 잔여 컨피그레이션 또는 크리덴셜 데이터가 남아 있지 않으며, 디바이스를 안전하게 보호하여 다시 온보딩할 수 있습니다. 보안 관련 공장 재설정의 경우, 재온보딩 중에 새 자격 증명(비밀번호, 키, 인증서)이 생성되고 사전 보안 침해 백업 컨피그레이션이 디바이스에 복원되지 않는지 확인합니다.

Q: 대신 "request platform software sdwan software reset" 또는 "request platform software sdwan config reset"을 사용하는 것은 어떻습니까?

A : 이러한 명령은 다른 목적을 제공하며 `factory-reset all secure`와 동일한 수준의 정화 기능을 제공하지 않습니다. 요청 플랫폼 소프트웨어 `sdwan software reset` 명령은 SD-WAN 소프트웨어 오버레이를 재설정하지만 기본 Cisco IOS XE 컨피그레이션, 키, 인증서 또는 스토리지는 지우지 않습니다. 디바이스는 기본 OS 상태를 유지합니다. 요청 플랫폼 소프트웨어 `sdwan config reset` 명령은 SD-WAN 컨피그레이션만 재설정하지만 Cisco IOS XE 이미지, 로컬 자격 증명, SSH 키 및 기타 모든 데이터는 디스크에 그대로 둡니다. 두 명령 모두 스토리지 미디어에 대한 데이터 삭제를 수행하지 않습니다. 디바이스를 완전 정상 상태로 되돌리는 것이 목표인 경우(특히 보안 사고 이후), 이러한 명령은 나머지 데이터(키, 자격 증명, 로그, 공격자가 심은 파일)가 플래시 또는 SSD에 남아 있을 수 있기 때문에 충분하지 않습니다. 스토리지 레벨에서 디바이스를 정상 상태로 유지해야 하는 경우 공장 초기화 모든 보안 설정을 사용합니다.

참조

- Cisco Trustworthy Systems — 공장 초기화 가이드
- Cisco Edge 라우터에 HSECK9 라이센스 구성
- Cisco Catalyst SD-WAN에서 HSEC 라이센스 관리
- CLI를 사용하여 부트스트랩 파일 생성 — SD-WAN 시작 가이드
- vManage GUI 또는 CLI를 사용하여 SD-WAN 컨트롤러 업그레이드

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.