Voer een Secure Factory Reset uit op SD-WAN cEdge Routers

Inhoud

Inleiding

In dit document wordt de procedure voor het veilig terugzetten van fabrieksinstellingen beschreven voor Cisco Catalyst SD-WAN Edge Routers waarop Cisco IOS® XE wordt uitgevoerd.

Achtergrond

Een fabrieksreset brengt het apparaat terug naar de oorspronkelijke productietoestand en is meestal vereist als onderdeel van de werkstromen voor uitbedrijfname, herimplementatie of herstel van de beveiliging.

⚠ Waarschuwing: Dit artikel beveelt uitsluitend de `fabrieksreset alle beveiligde` optie, die data sanitatie uitvoert in lijn met NIST SP 800-88 Rev. 1. Deze methode maakt gegevens op opslagmedia onherstelbaar en biedt de hoogste mate van zekerheid dat gevoelige gegevens permanent zijn verwijderd.

toepasbaarheid

De `fabrieksreset voor alle beveiligde` opdrachten wordt ondersteund op deze platforms waarop Cisco IOS XE wordt uitgevoerd:

- Cisco Catalyst 8200-reeks Edge-platforms
- Cisco Catalyst 8300-reeks Edge-platforms
- Cisco Catalyst 8500-reeks Edge-platforms
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco ISR 1000 Series Integrated Services Routers

✎ Opmerking: de `optie All Secure` kan alleen worden gebruikt op zelfstandige apparaten. Controleer of uw platform en de Cisco IOS XE-versie het `veilige` trefwoord ondersteunt door `fabrieksreset ?` in de geprivilegieerde EXEC-modus te controleren voordat u verdergaat.

Voorwaarden

Voordat u de veilige fabrieksreset uitvoert, moet u controleren of aan de volgende voorwaarden is voldaan:

- Back-upconfiguratie: Exporteer en sla alle apparaatconfiguraties, sjablonen en beleidsregels veilig op vanuit de SD-WAN Manager (vManage) voordat u deze opnieuw instelt.
- Back-up van software-images: Zorg ervoor dat u een kopie van de software-image van Cisco IOS XE in bootflash hebt geladen voordat u de reset uitvoert. Hoewel de `veilige` optie op de meeste platforms het opstartimage in flash behoudt, ontsmetten bepaalde platforms bootflash volledig als onderdeel van de veilige wissing. Als noodgeval moet u altijd de Cisco IOS XE-image beschikbaar hebben op een USB-station of toegankelijke TFTP-server om herstel te garanderen, ongeacht het gedrag van het platform.
- Ononderbroken voeding: Zorg ervoor dat het apparaat gedurende het hele resetproces een ononderbroken voeding heeft. Stroomverlies tijdens reiniging kan het apparaat onherstelbaar

maken.

- Alle ISSU-procedures voltooien: Als er in-Service Software Upgrade (ISSU)-bewerkingen in behandeling zijn of worden uitgevoerd, voltooit u deze voordat u de fabrieksreset start.
- HSEC-licentie vrijgeven: de HSEC-licentie moet worden vrijgegeven van het apparaat voordat de fabrieksreset wordt uitgevoerd. De HSECK9-licentie retourneren zoals beschreven in het gedeelte "De HSECK9-licentie retourneren" op: HSECK9-licentie configureren op Cisco Edge Routers
- Verwijderen uit SD-WAN Fabric: het apparaatcertificaat van vManage ongeldig maken en het apparaat verwijderen uit de controlleroverlay voordat u de reset uitvoert.
- Consoletoegang: Zorg ervoor dat u fysieke consoletoegang hebt tot het apparaat. Na de reset gaat het apparaat over naar de ROMMON-modus en zijn VTY-sessies niet beschikbaar.

Tip: Bevestig dat het Cisco IOS XE-image in bootflash is geladen en dat er een herstelkopie beschikbaar is op USB of TFTP voordat de fabrieksreset wordt uitgevoerd. Hoewel de `veilige` optie op de meeste platforms het opstartimage behoudt, ontsmetten sommige platforms bootflash volledig tijdens het proces.

Wat wordt gewist

Met de `fabrieksreset voor alle beveiligde` opdrachten worden deze gegevens permanent van het apparaat verwijderd:

Rubriek	Gegevens gewist
in Cisco IOS®-software	Alle software-images van Cisco IOS XE (het huidige opstartimage wordt op de meeste platforms in Flash bewaard, maar op bepaalde platforms wordt bootflash volledig gedesinfecteerd)
Configuratie	Opstartconfiguratie, actieve configuratie
Logboeken en diagnostiek	Crashinformatie, systeemlogboeken, OBFL (On-Board Failure Logging)
beveiligingsmateriaal	FIPS-gerelateerde sleutels en referenties, door de gebruiker geconfigureerde PKI-sleutels en certificaten
opslag	Alle gebruikersgegevens op verwisselbare opslag (SATA, SSD, USB)
vergunning	Alle apparaatlicenties (opnieuw registreren vereist)
ROMmon	Door de gebruiker toegevoegde ROMON-omgevingsvariabelen

---

Opmerking: deze items worden bewaard na de veilige fabrieksreset:

- SUDI (Secure Unique Device Identifier)-certificaten en bijbehorende PKI-sleutels
- Configuratieregisterwaarde

- Het huidige opstartbeeld (bewaard in flash op de meeste platforms; op bepaalde platforms is bootflash volledig ontsmet - altijd USB / TFTP-herstel geënsceneerd)

Procedure: Beveiligde fabrieksreset

Waarschuwing: deze procedure is onomkeerbaar. Na het opstarten worden alle gegevens in de vorige tabel permanent vernietigd. Controleer of alle back-ups zijn geverifieerd voordat u doorgaat.

Stap 1: Toegang tot het apparaat via de console

Maak verbinding met het apparaat via een fysieke consoleverbinding. SSH/VTY-toegang gaat verloren tijdens het resetproces.

Stap 2: Voer de geprivilegieerde EXEC-modus in

```
Device> enable
Device#
```

Stap 3: Voer de Secure Factory Reset uit

Voer deze opdracht uit om de veilige fabrieksreset te starten:

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

Het systeem vraagt om bevestiging:

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

Controleren: controleer bij de bevestigingsprompt een laatste keer dat:

- Van alle configuraties is een back-up gemaakt
- De Cisco IOS XE-herstelimage is beschikbaar op USB of TFTP
- Het apparaat is verwijderd uit de SD-WAN-overlay

Typ `y` of druk op Enter om te bevestigen en ga verder.

Stap 4: Wacht tot de reiniging is voltooid

Het apparaat voert gegevensreiniging uit op alle opslagmedia. Dit proces kan een langere periode in beslag nemen, afhankelijk van de opslagcapaciteit. Onderbreek de stroomtoevoer niet tijdens deze bewerking.

Na voltooiing laadt het apparaat automatisch opnieuw en gaat het in de ROMMON-modus.

Stap 5: ROMON-omgevingsvariabelen herstellen

Na de reset kunnen omgevingsvariabelen zoals `MAC_ADDRESS` en `SERIAL_NUMBER` gewist worden. Voer een ROMMON-reset uit om ze te herstellen:

```
rommon 1> reset
```

Opmerking: De omgevingsvariabele BAUD-rente keert na een fabrieksreset terug naar de standaardwaarde (9600). Als uw consolesessie met een andere baud-snelheid is geconfigureerd, kunt u de instellingen van de terminalemulator aanpassen naar 9600 baud om weer toegang tot de console te krijgen.

Stap 6: Start de Cisco IOS XE Software Image op

Op de meeste platforms behoudt de `veilige` optie het opstartbeeld in Flash. Controleer de aanwezigheid ervan met `dir bootflash:` van ROMMON. Als het image beschikbaar is, start u direct op:

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

Platformspecifiek gedrag: Op bepaalde hardwareplatforms wordt bootflash volledig gewist door het veilige reinigingsproces, inclusief het opstartbeeld. Herstel in deze gevallen via USB of TFTP.

Optie A — USB-herstel:

```
rommon 2> boot usbflash0:<image-filename>.bin
```

Optie B — TFTP-herstel:

Stel de vereiste ROMON-omgevingsvariabelen in en start de overdracht:

```
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
```

Controleren of de verbinding met de TFTP-server beschikbaar is via de beheerinterface of via een direct aangesloten netwerksegment. ROMMON ondersteunt geen routeringsprotocollen, dus de TFTP-server moet bereikbaar zijn via de geconfigureerde standaardgateway.

Zorg ervoor dat er altijd een herstelimage op USB of een toegankelijke TFTP-server is geënsceneerd voordat u de fabrieksreset start om dit gedrag te verklaren.

Post-Reset: opnieuw aan boord van SD-WAN-verbinding

Nadat het apparaat is hersteld met een schone Cisco IOS XE-image, gebruikt u standaard SD-WAN-onboarding-procedures om het apparaat terug in de fabric te brengen:

1. Bootstrap-configuratie: Pas de initiële bootstrap-configuratie toe (systeem-IP, site-ID,

organisatienaam, vBond-adres). Raadpleeg Bootstrap-bestand genereren met CLI voor de procedure.
2. Installatie van certificaat: installeer het apparaatcertificaat en de CA-hoofdketen zoals vereist door uw certificeringsinstantie (Symantec/DigiCert, Cisco PKI of Enterprise CA).
3. Controleverbindingen: Controleer of DTLS/TLS-besturingsverbindingen zijn gemaakt voor vManage, vSmart en vBond.
4. Sjabloon Push: vanuit vManage koppelt u de juiste apparaatsjabloon of configuratiegroep aan het apparaat.
5. Validatie: Bevestig dat BFD-sessies, OMP-routes en tunnels voor gegevensvliegtuigen operationeel zijn.

Opmerking: na het opnieuw instappen moet de HSEC-licentie (High Security) handmatig opnieuw worden toegepast via CLI om de crypto-doorvoer te herstellen. Zoals gedocumenteerd in Beheer van HSEC-licenties in Cisco Catalyst SD-WAN, ondersteunt SD-WAN Manager (vManage) niet het opnieuw installeren van een HSEC-licentie op een apparaat. Het opnieuw laden van het apparaat is vereist op fysieke routers om de licentie te activeren. Raadpleeg HSECK9-licentie configureren op Cisco Edge Routers voor de handmatige CLI-procedure.

Probleemoplossing

Console reageert niet na reset

Als de console niet reageert nadat de fabrieksreset is voltooid, is de baud-snelheid waarschijnlijk weer de standaardwaarde (9600). Stel de terminalemulator in op 9600 baud en sluit deze opnieuw aan.

Apparaat komt niet in ROMMON

Als het apparaat geen ROMON invoert nadat de reset is voltooid, controleert u of het configuratieregister correct is ingesteld. In de meeste gevallen dwingt een stroomcyclus het apparaat in ROMMON wanneer er geen opstartbaar beeld aanwezig is.

Ontbrekende omgevingsvariabelen in ROMON

Als variabelen `MAC_ADDRESS` of `SERIAL_NUMBER` ontbreken na de reset, geeft u de opdracht `Reset` in ROMON op om de fabrieksinstellingen-standaardomgevingsvariabelen van de hardwareopslag te herstellen.

Veelgestelde vragen

V: Waarom wordt de "veilige" optie aanbevolen boven de standaard "alle" of "3-pass" opties?

A: De `fabrieksreset alle beveiligde` optie voert de meest grondige data sanering beschikbaar, afgestemd op NIST SP 800-88 Rev. 1. Het maakt gegevens onherstelbaar en behoudt de huidige opstartimage in Flash, waardoor herstel wordt vereenvoudigd. Ter vergelijking: de optie `3-pass` voert een drievoudig overschrijfpatroon uit (nullen, enen, willekeurig) dat ongeveer drie keer langer duurt en ook het opstartbeeld wist, waardoor een volledige image opnieuw moet worden geladen van USB of TFTP. De `veilige` optie wordt aanbevolen omdat deze de meest grondige reiniging biedt met de minste operationele overhead voor herstel.

V: Hoe lang duurt de veilige fabrieksreset?

A: De duur varieert op basis van de totale opslagcapaciteit van het apparaat. Voor apparaten met standaard flashopslag (8-32 GB) wordt het proces doorgaans binnen 15-45 minuten voltooid. Apparaten met grotere SSD- of SATA-opslag kunnen langer duren. Belangrijk: Onderbreek de stroom niet tijdens dit proces. Plan een onderhoudvenster waarin rekening wordt gehouden met de reset plus de tijd voor het opnieuw laden en inschakelen van het image.

V: Behoudt het apparaat zijn identiteit (serienummer, SUDI) na de reset?

A: Ja. Het Secure Unique Device Identifier (SUDI)-certificaat en de bijbehorende PKI-sleutels worden opgeslagen in een hardware-beveiligde opslag (TAm/ACT2-chip) en worden niet gewist door de fabrieksreset. Het serienummer van het apparaat wordt ook bewaard in de hardware. Dit betekent dat het apparaat na de reset opnieuw aan boord van de SD-WAN-verbinding kan worden gebracht met behulp van de oorspronkelijke identiteit.

V: Moet ik het apparaat uit SD-WAN Manager verwijderen voordat ik de reset kan uitvoeren?

A: Ja. Het wordt ten zeerste aanbevolen om het apparaatcertificaat ongeldig te maken en het apparaat uit de SD-WAN-overlay te verwijderen voordat u de fabrieksreset uitvoert. Dit zorgt voor een schone verwijdering van de controllerinfrastructuur, geen verouderde vermeldingen in de inventaris van vManage-apparaten en geen verweesde besturingsverbindingen of tunnelstatus. Van vManage: Navigeer naar Configuratie > Certificaten > selecteer het apparaat > Ongeldig maken en Verzend naar Controllers. Verwijder het apparaat vervolgens uit de apparaatlijst.

V: Wat gebeurt er met de HSEC-licentie na de fabrieksreset?

A: De HSEC-licentie (High Security) wordt verwijderd tijdens de fabrieksreset. Zonder dit werkt het

apparaat met een beperkte crypto-doorvoer. De HSEC-licentie moet worden vrijgegeven voordat de fabrieksreset wordt uitgevoerd, zodat deze achteraf opnieuw kan worden gebruikt:

1. Vóór reset: de licentie vrijgeven via `slimme licentieautorisatie, lokaal online retourneren` en de productinstantie verwijderen uit Smart License Central.
2. Na re-onboarding: de HSEC-licentie handmatig opnieuw toepassen via CLI. Zoals beschreven in Beheer van HSEC-licenties in Cisco Catalyst SD-WAN, biedt SD-WAN Manager (vManage) geen ondersteuning voor het opnieuw installeren van de HSEC-licentie.
3. Opnieuw laden: op fysieke routers is opnieuw laden vereist om de licentie te activeren.
4. Verifieer via `licentieoverzicht tonen` en `licentieautorisatie tonen`.

Raadpleeg Configure HSECK9 License on Cisco Edge Routers en Managing HSEC Licenses in Cisco Catalyst SD-WAN voor de volledige procedure.

V: Kan ik de veilige fabrieksreset op afstand uitvoeren (via SSH/VTY)?

A: Hoewel het commando technisch kan worden uitgegeven via een SSH / VTY-sessie, wordt het sterk afgeraden. Het apparaat begint onmiddellijk met de reiniging en de sessie op afstand wordt beëindigd. Na de reset komt het apparaat in de ROMMON-modus waar geen IP-connectiviteit beschikbaar is, geen VTY-toegang mogelijk is en consoletoegang vereist is voor imageherstel. Zorg er altijd voor dat de fysieke console beschikbaar is voordat u de fabrieksreset start.

V: Is de veilige fabrieksreset geschikt voor scenario's voor beveiligingsherstel?

A: Ja. De veilige fabrieksreset is de aanbevolen aanpak wanneer een apparaat moet worden teruggebracht naar een bekende goede staat na een vermoedelijk compromis. Dit zorgt ervoor dat alle door de aanvaller geplante sleutels, backdoors of persistentiemechanismen permanent worden verwijderd, er geen resterende configuratie- of aanmeldingsgegevens overblijven en het apparaat gegarandeerd schoon is voor opnieuw instappen. Voor fabrieksresets met betrekking tot beveiliging moet u ervoor zorgen dat nieuwe referenties (wachtwoorden, sleutels, certificaten) worden gegenereerd tijdens het opnieuw aan boord gaan en dat er geen back-upconfiguraties worden teruggezet naar het apparaat die vooraf zijn gecompromitteerd.

V: Waarom zou u in plaats daarvan "reset van de sdwan-software voor het aanvraagplatform" of "reset van de sdwan-configuratie voor het aanvraagplatform" gebruiken?

A: Deze opdrachten dienen een ander doel en bieden niet hetzelfde niveau van reiniging als `fabrieksreset allemaal veilig`. Met de opdracht `Software resetten van` de aanvraagsoftware wordt de SD-WAN-software-overlay opnieuw ingesteld, maar worden de onderliggende Cisco IOS XE-configuraties, sleutels, certificaten of opslag niet gewist. Het apparaat behoudt de status van het basisbesturingssysteem. Met de opdracht `request platform software sdwan config reset` wordt alleen de SD-WAN-configuratie gereset, maar blijven de Cisco IOS XE-image, lokale referenties,

SSH-sleutels en alle andere gegevens intact op de schijf. Geen van beide opdrachten voert gegevensreiniging uit op de opslagmedia. Als het doel is om het apparaat terug te brengen naar een volledig schone staat - vooral na een beveiligingsincident - zijn deze opdrachten onvoldoende omdat resterende gegevens (sleutels, referenties, logs, door aanvallers geplante bestanden) op flash of SSD kunnen blijven. Gebruik `fabrieksreset voor alle veilige` apparaten wanneer het apparaat gegarandeerd schoon moet zijn op opslagniveau.

Referenties

- Betrouwbare systemen van Cisco — Handleiding voor fabrieksreset
- HSECK9-licentie configureren op Cisco Edge-routers
- HSEC-licenties beheren in Cisco Catalyst SD-WAN
- Bootstrap-bestand genereren met behulp van CLI — Handleiding voor starten met SD-WAN
- Upgrade SD-WAN-controllers met behulp van vManage GUI of CLI

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.