Sicheres Zurücksetzen auf SD-WAN-cEdge-Router ab Werk

Inhalt

Einleitung

In diesem Dokument wird das sichere Zurücksetzen auf die Werkseinstellungen für Cisco Catalyst SD-WAN Edge-Router mit Cisco IOS® XE beschrieben.

Hintergrund

Ein Zurücksetzen auf die Werkseinstellungen setzt das Gerät auf den ursprünglichen Fertigungszustand zurück und ist in der Regel für die Stilllegung, die Neubereitstellung oder für die Sicherheitsbehebung erforderlich.

⚠ Vorsicht: In diesem Artikel wird ausschließlich die `werksseitig zurückgesetzte` Option `All Secure` empfohlen, die eine Datenbereinigung in Übereinstimmung mit NIST SP 800-88 Rev. 1 durchführt. Diese Methode macht Daten auf Speichermedien nicht wiederherstellbar und bietet die höchste Sicherheit, dass vertrauliche Daten dauerhaft entfernt wurden.

Geltungsbereich

Der Befehl `"Alle sicheren` Werkseinstellungen zurücksetzen" wird auf den folgenden Plattformen mit Cisco IOS XE unterstützt:

- Cisco Catalyst Edge-Plattformen der Serie 8200
- Cisco Catalyst Edge-Plattformen der Serie 8300
- Cisco Catalyst Edge-Plattformen der Serie 8500
- Cisco Aggregation Services Router der Serie ASR 1000
- Cisco Integrated Services Router der Serie ISR 4000
- Cisco Integrated Services Router der Serie ISR 1000

✎ Anmerkung: Die Option `all secure` kann nur auf Einzelgeräten verwendet werden. Stellen Sie sicher, dass Ihre Plattform und die Cisco IOS XE-Version das `sichere` Schlüsselwort unterstützen, indem Sie `Zurücksetzen auf die Werkseinstellungen` aktivieren. im privilegierten EXEC-Modus, bevor Sie fortfahren.

Voraussetzungen

Bevor Sie das sichere Zurücksetzen auf die Werkseinstellungen durchführen, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Sicherungskonfiguration: Exportieren Sie alle Gerätekonfigurationen, Vorlagen und Richtlinien aus dem SD-WAN-Manager (vManage), und speichern Sie sie vor dem Zurücksetzen sicher.
- Sicherungssoftware-Images: Stellen Sie sicher, dass Sie eine Kopie des Cisco IOS XE Software-Images in den Bootflash geladen haben, bevor Sie das Zurücksetzen durchführen. Während die Option `secure` das Boot-Image im Flash auf den meisten Plattformen beibehält, säubern bestimmte Plattformen bootflash vollständig als Teil der sicheren Zurücksetzung. Halten Sie das Cisco IOS XE-Image grundsätzlich auf einem USB-Laufwerk oder einem TFTP-Server bereit, auf den zugegriffen werden kann, um eine Wiederherstellung

unabhängig vom Plattformverhalten zu gewährleisten.

- Unterbrechungsfreie Stromversorgung: Stellen Sie sicher, dass das Gerät während des gesamten Reset-Vorgangs über eine unterbrechungsfreie Stromversorgung verfügt. Ein Stromverlust während der Desinfektion kann dazu führen, dass das Gerät nicht wiederhergestellt werden kann.
- Führen Sie alle ISSU-Verfahren aus: Wenn In-Service-Software-Upgrades (ISSU) ausstehen oder ausgeführt werden, führen Sie diese durch, bevor Sie das Zurücksetzen auf die Werkseinstellungen starten.
- HSEC-Lizenz freigeben: Die HSEC-Lizenz muss vom Gerät freigegeben werden, bevor das Gerät auf die Werkseinstellungen zurückgesetzt wird. Senden Sie die HSECK9-Lizenz wie im Abschnitt "Return the HSECK9 License" (HSECK9-Lizenz zurückgeben) unter: Konfigurieren der HSECK9-Lizenz für Cisco Edge-Router beschrieben zurück.
- Aus SD-WAN-Fabric entfernen: Deaktivieren Sie das Gerätezertifikat von vManage, und entfernen Sie das Gerät aus dem Controller-Overlay, bevor Sie das Zurücksetzen durchführen.
- Konsolenzugriff: Stellen Sie sicher, dass Sie über eine physische Konsole auf das Gerät zugreifen können. Nach dem Zurücksetzen wechselt das Gerät in den ROMMON-Modus, und VTY-Sitzungen sind nicht verfügbar.

Tipp: Vergewissern Sie sich, dass das Cisco IOS XE-Image in den Bootflash geladen wurde und dass eine Wiederherstellungskopie auf USB oder TFTP verfügbar ist, bevor Sie das Zurücksetzen auf die Werkseinstellungen durchführen. Während die `sichere` Option das Boot-Image auf den meisten Plattformen beibehält, wird Bootflash auf einigen Plattformen vollständig bereinigt.

Was wird gelöscht?

Mit dem Befehl `"Alle sicheren` Einstellungen auf `Werkseinstellungen zurücksetzen`" werden diese Daten dauerhaft vom Gerät entfernt:

Kategorie	Daten gelöscht
Software	Alle Cisco IOS XE Software-Images (das aktuelle Boot-Image wird auf den meisten Plattformen im Flash-Speicher beibehalten. bootflash wird jedoch auf bestimmten Plattformen vollständig bereinigt)
Konfiguration	Startkonfiguration, aktuelle Konfiguration
Protokolle und Diagnose	Absturzinformationen, Systemprotokolle, OBFL (On-Board Failure Logging)
Sicherheitsmaterial	FIPS-bezogene Schlüssel und Anmeldedaten, vom Benutzer konfigurierte PKI-Schlüssel und Zertifikate
Storage	Alle Benutzerdaten auf Wechseldatenträger (SATA, SSD, USB)
Lizenzierung	Alle Gerätelizenzen (erneute Registrierung erforderlich)
ROMMON	Benutzerdefinierte ROMMON-Umgebungsvariablen

Anmerkung: Diese Elemente werden nach dem sicheren Zurücksetzen auf die Werkseinstellungen beibehalten:

- SUDI-Zertifikate (Secure Unique Device Identifier) und zugehörige PKI-Schlüssel
- Konfigurationsregisterwert
- Das aktuelle Boot-Image (wird auf den meisten Plattformen im Flash-Speicher beibehalten; auf bestimmten Plattformen ist bootflash vollständig bereinigt - immer USB/TFTP-Wiederherstellung bereitgestellt)

Vorgehensweise: Sicheres Zurücksetzen auf Werkseinstellungen

Warnung: Dieses Verfahren ist unumkehrbar. Nach der Initiierung werden alle in der vorherigen Tabelle aufgeführten Daten endgültig gelöscht. Stellen Sie sicher, dass alle Sicherungen überprüft wurden, bevor Sie fortfahren.

Schritt 1: Zugriff auf das Gerät über die Konsole

Stellen Sie über eine physische Konsolenverbindung eine Verbindung mit dem Gerät her. Der SSH-/VTY-Zugriff geht beim Zurücksetzen verloren.

Phase 2: privilegierten EXEC-Modus eingeben

```
Device> enable
Device#
```

Schritt 3: Secure Factory Reset durchführen

Führen Sie den folgenden Befehl aus, um das sichere Zurücksetzen auf die Werkseinstellungen zu initiieren:

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

Das System fordert Sie zur Bestätigung auf:

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

Überprüfen: Überprüfen Sie abschließend bei der Bestätigungsaufforderung Folgendes:

- Alle Konfigurationen wurden gesichert.
- Das Cisco IOS XE Wiederherstellungs-Image ist auf USB oder TFTP verfügbar.
- Das Gerät wurde aus dem SD-WAN-Overlay entfernt.

Geben Sie `y ein`, oder drücken Sie die Eingabetaste, um die Eingabe zu bestätigen und fortzufahren.

Schritt 4: Warten, bis die Bereinigung abgeschlossen ist

Das Gerät führt die Datenbereinigung auf allen Speichermedien durch. Dieser Vorgang kann je nach Speicherkapazität einen längeren Zeitraum in Anspruch nehmen. Unterbrechen Sie während dieses Vorgangs nicht die Stromversorgung.

Nach Abschluss lädt das Gerät automatisch neu und wechselt in den ROMMON-Modus.

Schritt 5: ROMMON-Umgebungsvariablen wiederherstellen

Nach dem Zurücksetzen können Umgebungsvariablen wie `MAC_ADDRESS` und `SERIAL_NUMBER` gelöscht werden. Führen Sie ein ROMMON-Reset durch, um sie wiederherzustellen:

```
rommon 1> reset
```

Anmerkung: Die Umgebungsvariable BAUD rate kehrt nach einem Zurücksetzen auf die Werkseinstellungen auf ihren Standardwert (9600) zurück. Wenn Ihre Konsolensitzung mit einer anderen Baudrate konfiguriert wurde, können Sie die Terminalemulationseinstellungen auf 9600 Baud einstellen, um wieder Konsolenzugriff zu erhalten.

Schritt 6: Booten des Cisco IOS XE Software-Images

Auf den meisten Plattformen behält die `sichere` Option das Boot-Image im Flash bei. Vergewissern Sie sich mithilfe von `dir bootflash:` von ROMMON. Wenn das Image verfügbar ist, starten Sie direkt:

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

> Plattformspezifisches Verhalten: Auf bestimmten Hardwareplattformen löscht der sichere Bereinigungsprozess den Bootflash vollständig, einschließlich des Boot-Images. In diesen Fällen erfolgt die Wiederherstellung über USB oder TFTP.
>
> Option A — USB-Wiederherstellung:
>
> ```
> rommon 2> boot usbflash0:<image-filename>.bin
> ```
>
> Option B - TFTP-Wiederherstellung:
>
> Stellen Sie die erforderlichen ROMMON-Umgebungsvariablen ein, und starten Sie dann den Transfer:
>
> ```
> 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
> ```
>
> Überprüfen Sie, ob die Verbindung zum TFTP-Server über die Verwaltungsschnittstelle oder ein direkt verbundenes Netzwerksegment verfügbar ist. ROMMON unterstützt keine Routing-Protokolle, daher muss der TFTP-Server über das konfigurierte Standard-Gateway erreichbar sein.
>
> Lassen Sie immer ein Wiederherstellungs-Image auf USB oder einem zugänglichen TFTP-

> Server bereitstellen, bevor Sie das Zurücksetzen auf die Werkseinstellungen starten, um dieses Verhalten zu berücksichtigen.

Nach dem Zurücksetzen: Re-Onboarding zur SD-WAN-Fabric

Nachdem das Gerät mit einem sauberen Cisco IOS XE-Image wiederhergestellt wurde, verwenden Sie die standardmäßigen SD-WAN-Integrationsverfahren, um das Gerät wieder in die Fabric einzubinden:

1. Bootstrap-Konfiguration: Anwenden der anfänglichen Bootstrap-Konfiguration (System-IP, Standort-ID, Organisationsname, vBond-Adresse) Informationen zum Verfahren finden Sie unter Generate Bootstrap File Using CLI (Bootstrap-Datei mit CLI generieren).
2. Installation des Zertifikats: Installieren Sie das Gerätezertifikat und die Stammzertifizierungsstellenkette, wie von Ihrer Zertifizierungsstelle (Symantec/DigiCert, Cisco PKI oder Enterprise CA) gefordert.
3. Steuerverbindungen: Überprüfen Sie, ob die DTLS/TLS-Steuerverbindungen zu vManage, vSmart und vBond hergestellt sind.
4. Vorlagen-Push: Hängen Sie unter vManage die entsprechende Gerätevorlage oder Konfigurationsgruppe an das Gerät an.
5. Validierung: Bestätigung, dass BFD-Sitzungen, OMP-Routen und Tunnel auf Datenebene betriebsbereit sind

---

Anmerkung: Nach dem Re-Onboarding muss die HSEC-Lizenz (High Security) manuell über die CLI erneut angewendet werden, um den Krypto-Durchsatz wiederherzustellen. Wie unter Verwalten von HSEC-Lizenzen im Cisco Catalyst SD-WAN dokumentiert, unterstützt SD-WAN Manager (vManage) nicht die Neuinstallation einer HSEC-Lizenz auf einem Gerät. Auf physischen Routern muss das Gerät neu geladen werden, um die Lizenz zu aktivieren. Informationen zum manuellen CLI-Verfahren finden Sie unter Konfigurieren der HSECK9-Lizenz auf Cisco Edge-Routern.

Fehlerbehebung

Konsole reagiert nach Zurücksetzen nicht

Wenn die Konsole nach Abschluss des Zurücksetzens auf die Werkseinstellungen nicht mehr reagiert, ist die Baudrate wahrscheinlich auf den Standardwert (9600) zurückgegangen. Stellen Sie den Terminal-Emulator auf 9600 Baud ein, und schließen Sie ihn erneut an.

Gerät gibt ROMMON nicht ein

Wenn das Gerät nach Abschluss des Resets nicht ROMMON aufruft, stellen Sie sicher, dass das Konfigurationsregister richtig eingestellt ist. In den meisten Fällen zwingt ein Ein-/Ausschaltzyklus das Gerät zu ROMMON, wenn kein bootfähiges Image vorhanden ist.

Fehlende Umgebungsvariablen in ROMMON

Wenn die Variablen `MAC_ADDRESS` oder `SERIAL_NUMBER` nach dem Zurücksetzen fehlen, führen Sie den Befehl `reset` in ROMMON aus, um die werkseitigen Umgebungsvariablen aus dem Hardwarespeicher wiederherzustellen.

Häufig gestellte Fragen

F: Warum wird die Option "Sicher" gegenüber den Standardoptionen "Alle" oder "3 Durchgänge" empfohlen?

A : Die Option `Alle sicheren` Daten auf die Werkseinstellungen zurücksetzen führt die gründlichste verfügbare Datenbereinigung durch, die auf NIST SP 800-88 Rev. 1 abgestimmt ist. Sie macht Daten nicht wiederherstellbar und behält das aktuelle Boot-Image im Flash bei, was die Wiederherstellung vereinfacht. Im Vergleich dazu führt die `3-Pass`-Option ein 3-Pass-Überschreibmuster (Nullen, Einsen, zufällig) durch, das etwa dreimal länger dauert und auch das Boot-Image löscht, sodass ein vollständiges Image von USB oder TFTP neu geladen werden muss. Die `sichere` Option wird empfohlen, da sie die gründlichste Bereinigung mit dem geringsten betrieblichen Aufwand für die Wiederherstellung bietet.

F: Wie lange dauert das sichere Zurücksetzen auf die Werkseinstellungen?

A : Die Dauer hängt von der gesamten Speicherkapazität des Geräts ab. Bei Geräten mit standardmäßigem Flash-Speicher (8-32 GB) dauert dieser Vorgang in der Regel 15-45 Minuten. Geräte mit größeren SSD- oder SATA-Speichern können länger dauern. Wichtig: Unterbrechen Sie während dieses Vorgangs nicht die Stromversorgung. Planen Sie ein Wartungsfenster, in dem das Zurücksetzen, das erneute Laden und Wiedereingliedern von Bildern berücksichtigt ist.

F: Behält das Gerät nach dem Zurücksetzen seine Identität (Seriennummer, SUDI) bei?

A : Ja. Das Secure Unique Device Identifier (SUDI)-Zertifikat und die zugehörigen PKI-Schlüssel werden in einem hardwaregeschützten Speicher (TAm/ACT2-Chip) gespeichert und nicht durch Zurücksetzen auf die Werkseinstellungen gelöscht. Die Seriennummer des Geräts bleibt ebenfalls

in der Hardware erhalten. Das bedeutet, dass das Gerät nach dem Zurücksetzen mithilfe seiner ursprünglichen Identität in die SD-WAN-Fabric reintegriert werden kann.

F: Muss ich das Gerät aus dem SD-WAN-Manager entfernen, bevor ich es zurücksetzen kann?

A : Ja. Es wird dringend empfohlen, das Gerätezertifikat ungültig zu machen und das Gerät aus dem SD-WAN-Overlay zu entfernen, bevor das Zurücksetzen auf die Werkseinstellungen durchgeführt wird. Dadurch wird sichergestellt, dass keine veralteten Einträge im Inventar der vManage-Geräte und keine verwaisten Steuerverbindungen oder der Tunnelstatus entfernt werden. Von vManage: Navigieren Sie zu Configuration > Certificates > wählen Sie das Gerät aus > Invalidate, und senden Sie es an Controller. Löschen Sie anschließend das Gerät aus der Geräteliste.

F: Was passiert mit der HSEC-Lizenz nach dem Zurücksetzen auf die Werkseinstellungen?

A : Die HSEC-Lizenz (High Security) wird beim Zurücksetzen auf die Werkseinstellungen entfernt. Andernfalls arbeitet das Gerät mit einem eingeschränkten Krypto-Durchsatz. Die HSEC-Lizenz muss vor dem Zurücksetzen auf die Werkseinstellungen freigegeben werden, damit sie anschließend wiederverwendet werden kann:

1. Vor dem Zurücksetzen: Lassen Sie die Lizenz über die `Smart-Autorisierung` der `Lizenz online verfügbar, und` entfernen Sie die Produktinstanz aus Smart License Central.
2. Nach dem Reboarding: Wenden Sie die HSEC-Lizenz über die CLI manuell erneut an. Wie unter Verwalten von HSEC-Lizenzen im Cisco Catalyst SD-WAN dokumentiert, unterstützt SD-WAN Manager (vManage) keine Neuinstallation der HSEC-Lizenz.
3. Neu laden: Physische Router müssen neu geladen werden, um die Lizenz zu aktivieren.
4. Überprüfen Sie dies mit `show license summary` und `show license authorization (Lizenzzusammenfassung anzeigen).`

Das vollständige Verfahren finden Sie unter Konfigurieren der HSECK9-Lizenz auf Cisco Edge-Routern und Verwalten von HSEC-Lizenzen im Cisco Catalyst SD-WAN.

F: Kann ich das sichere Zurücksetzen auf die Werkseinstellungen remote (über SSH/VTY) durchführen?

A : Technisch gesehen kann der Befehl zwar über eine SSH/VTY-Sitzung ausgegeben werden, es wird jedoch dringend davon abgeraten. Das Gerät beginnt sofort mit der Bereinigung, und die Remote-Sitzung wird beendet. Nach dem Zurücksetzen wechselt das Gerät in den ROMMON-Modus, wo keine IP-Verbindung verfügbar ist, kein VTY-Zugriff möglich ist und der Konsolenzugriff für die Image-Wiederherstellung erforderlich ist. Stellen Sie immer sicher, dass der Zugriff auf die physische Konsole möglich ist, bevor Sie das Zurücksetzen auf die Werkseinstellungen starten.

F: Ist die sichere Zurücksetzung auf die Werkseinstellungen für Szenarien mit Sicherheitsbehebung geeignet?

A : Ja. Das sichere Zurücksetzen auf die Werkseinstellungen wird empfohlen, wenn ein Gerät nach einer Kompromittierung in den zweifelsfrei funktionierenden Zustand zurückversetzt werden muss. Dadurch wird sichergestellt, dass alle von Angreifern platzierten Schlüssel, Backdoors oder Persistenzmechanismen dauerhaft entfernt werden, keine verbleibenden Konfigurations- oder Anmeldeinformationsdaten mehr vorhanden sind und das Gerät für das erneute Onboarding sicher sauber bleibt. Bei sicherheitsrelevanten Zurücksetzungen auf die Werkseinstellungen stellen Sie sicher, dass während des erneuten Onboarding neue Anmeldeinformationen (Kennwörter, Schlüssel, Zertifikate) generiert werden und dass keine kompromisslosen Backup-Konfigurationen auf dem Gerät wiederhergestellt werden.

F: Verwenden Sie stattdessen "request platform software sdwan software reset" oder "request platform software sdwan config reset".

A : Diese Befehle dienen einem anderen Zweck und bieten nicht das gleiche Maß an Bereinigung wie `werksseitiges Zurücksetzen alle sicher`. Der Befehl `request platform software sdwan software reset` setzt das SD-WAN-Software-Overlay zurück, löscht aber keine zugrunde liegenden Cisco IOS XE-Konfigurationen, -Schlüssel, -Zertifikate oder -Speicher - das Gerät behält seinen BS-Basisstatus. Mit dem Befehl `request platform software sdwan config reset` wird nur die SD-WAN-Konfiguration zurückgesetzt, das Cisco IOS XE-Image, die lokalen Anmeldeinformationen, die SSH-Schlüssel und alle anderen Daten bleiben jedoch auf der Festplatte erhalten. Keiner der beiden Befehle führt eine Datenbereinigung auf dem Speichermedium durch. Wenn das Ziel darin besteht, das Gerät in einen vollständig bereinigten Zustand zu versetzen - insbesondere nach einem Sicherheitsvorfall - sind diese Befehle unzureichend, da Restdaten (Schlüssel, Zugangsdaten, Protokolle, von Angreifern geplante Dateien) auf Flash oder SSD verbleiben können. Setzen Sie `alle Sicherheitseinstellungen auf die Werkseinstellungen zurück`, wenn das Gerät auf der Speicherebene sicher sauber sein muss.

Referenzen

- Cisco Trustworthy Systems - Leitfaden zum Zurücksetzen auf die Werkseinstellungen
- Konfigurieren der HSECK9-Lizenz auf Cisco Edge-Routern
- Verwalten von HSEC-Lizenzen im Cisco Catalyst SD-WAN
- Erstellen einer Bootstrap-Datei mit CLI - SD-WAN Erste Schritte
- Upgrade von SD-WAN-Controllern mithilfe der vManage-GUI oder -CLI

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.