在SD-WAN cEdge路由器上執行安全的出廠重置

目錄

簡介

本檔案介紹執行Cisco IOS® XE的Cisco Catalyst SD-WAN邊緣路由器的安全出廠重設程式。

背景

出廠重置將裝置返回到其原始製造狀態，通常作為停用、重新部署或安全補救工作流程的一部分需要。

⚠ 注意：本文僅推薦`factory-reset all secure`選項，該選項執行與NIST SP 800-88 Rev.1對齊的資料清理。此方法使儲存介質上的資料不可恢復，並提供永久刪除敏感資料的最高級別保證。

適用性

執行Cisco IOS XE的這些平台支援`factory-reset all secure`命令：

- Cisco Catalyst 8200系列邊緣平台
- Cisco Catalyst 8300系列邊緣平台
- Cisco Catalyst 8500系列邊緣平台
- Cisco ASR 1000系列聚合服務路由器
- Cisco ISR 4000系列整合式服務路由器
- Cisco ISR 1000系列整合式服務路由器

附註：`all secure`選項只能用於獨立裝置。通過檢查`factory-reset`，驗證您的平台和Cisco IOS XE版本是否支援`secure`關鍵字？進入特權執行模式，然後繼續。

必要條件

在執行安全出廠重置之前，請確保滿足以下前提條件：

- 備份配置：在重置之前，從SD-WAN Manager(vManage)匯出並安全地儲存所有裝置配置、模板和策略。
- 備份軟體映像：執行重置之前，請確保將Cisco IOS XE軟體映像的副本載入到bootflash中。雖然`secure`選項在大多數平台上都會在快閃記憶體中保留引導映像，但某些平台會將bootflash完全清理為安全擦除的一部分。作為一種應急措施，應始終在USB驅動器或可訪問的TFTP伺服器上提供Cisco IOS XE映像，以確保恢復不受平台行為的影響。
- 不間斷電源：確保裝置在整個重置過程中都有一個不間斷的電源。在清理過程中斷電可能導致裝置無法恢復。
- 完成所有ISSU過程：如果任何服務中軟體升級(ISSU)操作處於待定或進行中，請在啟動出廠重置之前完成這些操作。
- 版本HSEC許可證：執行出廠重置之前，必須從裝置中釋放HSEC許可證。 按照「返回HSECK9許可證」部分中的說明返回HSECK9許可證，該部分位於：在思科邊緣路由器上配置HSECK9許可證
- 從SD-WAN交換矩陣中刪除：執行重置之前，從vManage使裝置證書無效，並從控制器重疊中刪除裝置。
- 控制檯訪問：確保您擁有對裝置的物理控制檯訪問許可權。重置後，裝置進入ROMMON模式並且VTY會話不可用。

提示：執行出廠重設之前，請確認Cisco IOS XE映像已載入到bootflash ，並且USB或TFTP上有恢復副本可用。雖然`secure`選項在大多數平台上保留啟動映像，但某些平台會在

處理過程中完全清除bootflash。

擦除的內容

`factory-reset all secure`命令會永久從裝置中刪除此資料：

類別	資料已清除
軟體	所有Cisco IOS XE軟體映像(當前引導映像儲存在大多數平台的快閃記憶體中；但是，在某些平台上，bootflash完全經過清理)
組態	啟動配置，運行配置
日誌和診斷	崩潰資訊、系統日誌、OBFL（板載故障記錄）
安全資料	與FIPS相關的金鑰和憑證、使用者配置的PKI金鑰和證書
儲存	可移動儲存(SATA、SSD、USB)上的所有使用者資料
授權	所有裝置許可證（需要重新註冊）
ROMMON	使用者新增的ROMMON環境變數

附註：安全出廠重置後會保留以下專案：

- SUDI（安全唯一裝置識別符號）證書和關聯的PKI金鑰
- 配置暫存器值
- 目前開機映像(保留在大多數平台的快閃記憶體中；在某些平台上，bootflash已完全清理（始終暫存USB/TFTP恢復）

程序:安全出廠重置

警告：此過程是不可逆的。啟動後，永久銷毀上表中列出的所有資料。繼續之前，請確保所有備份都已驗證。

步驟 1:通過控制檯訪問裝置

通過物理控制檯連線連線到裝置。重置過程中會丟失SSH/VTY訪問。

步驟 2:進入特權執行模式

```
Device> enable
Device#
```

步驟 3:執行安全出廠重置

運行此命令以啟動安全出廠重置：

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

系統提示確認：

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

檢查:在確認提示時，最後一次驗證以下內容：

- 已備份所有配置
- Cisco IOS XE恢復映像可在USB或TFTP上使用
- 裝置已從SD-WAN重疊中刪除

鍵入y或按Enter以確認並繼續。

步驟 4:等待清理完成

該裝置對所有儲存介質執行資料清理。此過程可能需要較長的時間，具體取決於儲存容量。不要在此操作期間中斷電源。

完成後，裝置將自動重新載入並進入ROMMON模式。

步驟 5:恢復ROMMON環境變數

重置後，可以清除包括MAC_ADDRESS和SERIAL_NUMBER在內的環境變數。執行ROMMON重置以恢復它們：

```
rommon 1> reset
```

附註：出廠重置後，BAUD率環境變數返回其預設值(9600)。如果您的控制檯會話是以不同的波特率配置的，您可以將終端模擬器設定調整為9600波特以重新獲得控制檯訪問。

步驟 6:啟動Cisco IOS XE軟體映像

在大多數平台上，secure選項會保留快閃記憶體中的啟動映像。使用dir bootflash:來自ROMMON。如果映像可用，請直接啟動：

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

平台特定行為：在某些硬體平台上，安全清理過程會完全擦除bootflash，包括啟動映像。在這些情況下，請通過USB或TFTP進行恢復。

選項A — USB恢復：

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

選項B — TFTP復原：

設定所需的ROMMON環境變數，然後啟動傳輸：

```
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
```

> 驗證通過管理介面或直連網段與TFTP伺服器的連線是否可用。ROMMON不支援路由協定，因此TFTP伺服器必須通過配置的預設網關訪問。
>
> 在啟動出廠重置以解決此行為之前，請始終在USB 或可訪問的TFTP伺服器上暫存恢復映像。

重設後：重新註冊到SD-WAN交換矩陣

使用乾淨的Cisco IOS XE映像恢復裝置後，請使用標準SD-WAN自註冊過程將裝置重新引入交換矩陣：

1. 載入程式配置：應用初始載入程式配置（系統IP、站點ID、組織名稱、vBond地址）。 有關過程，請參閱使用CLI生成載入程式檔案。
2. 證書安裝：根據證書頒發機構（Symantec/DigiCert、Cisco PKI或企業CA）的要求安裝裝置證書和根CA鏈。
3. 控制連線：驗證是否已建立DTLS/TLS控制連線至vManage、vSmart和vBond。
4. 模板推送：在vManage中，將適當的裝置模板或配置組連線到裝置。
5. 驗證：確認BFD會話、OMP路由和資料平面隧道正常運行。

附註：重新登入後，必須通過CLI手動重新應用HSEC（高安全性）許可證以恢復加密吞吐量。如管理Cisco Catalyst SD-WAN中的HSEC許可證中所述，SD-WAN Manager(vManage)不支援在裝置上重新安裝HSEC許可證。在物理路由器上需要重新載入裝置才能啟用許可證。有關手動CLI過程，請參閱在思科邊緣路由器上配置HSECK9許可證。

疑難排解

控制檯在重置後無響應

如果控制檯在出廠重置完成後顯示無響應，波特率可能已恢復為預設值(9600)。 將終端模擬器調整為9600波特並重新連線。

裝置未進入ROMMON

如果裝置在重置完成後未進入ROMMON，請驗證配置暫存器設定正確。在大多數情況下，當沒有可引導映像時，電源循環會強制裝置進入ROMMON。

ROMMON中缺少環境變數

如果重置後缺少MAC_ADDRESS或SERIAL_NUMBER變數，請在ROMMON中發出reset命令以從硬體儲存恢復出廠預設的環境變數。

常見問題

Q:為什麼建議使用「安全」選項而不是標準的「全部」或「三通」選項？

A:factory-reset all secure選項執行可用的最徹底的資料清理，與NIST SP 800-88 Rev. 1保持一致。它使資料不可恢復並在快閃記憶體中保留當前啟動映像，從而簡化了恢復。相比之下，3通道選項執行三通道覆寫模式（零、一、隨機），大約需要三倍時間，同時也會清除開機映像，因此需要從USB或TFTP重新載入整個映像。建議使用secure選項，因為它提供了最徹底的衛生處理，並且恢復操作開銷最低。

Q:安全出廠重置需要多長時間？

A:持續時間因裝置的總儲存容量而異。對於具有標準快閃記憶體儲存(8-32 GB)的裝置，此過程通常在15-45分鐘內完成。具有較大的SSD或SATA儲存的裝置可能需要較長的時間。重要：在此過程中請勿中斷電源。規劃一個維護視窗，該視窗將考慮重置以及映像重新載入和重新加入時間。

Q:重置後，裝置是否保留其標識（序列號、SUDI）？

A:會。安全唯一裝置識別碼(SUDI)憑證及其相關PKI金鑰儲存在硬體保護儲存裝置(TAm/ACT2芯片)中，且不會被出廠重設清除。裝置序列號也儲存在硬體中。這意味著重置後，可以使用裝置的原始標識將該裝置重新註冊到SD-WAN交換矩陣。

Q:在執行重置之前，是否需要從SD-WAN Manager中刪除裝置？

A:會。強烈建議在執行出廠重置之前，使裝置證書無效並從SD-WAN重疊中刪除裝置。這可確保從控制器基礎架構中完全刪除、vManage裝置清單中無陳舊條目，以及無孤立控制連線或隧道狀態。在vManage中：導覽至Configuration > Certificates > select the device > Invalidate，然後導覽至Send to Controllers。然後，從裝置清單中刪除裝置。

Q:出廠重置後HSEC許可證會發生什麼情況？

A:在出廠重置期間刪除HSEC（高安全性）許可證。如果沒有此功能，裝置將以受限的加密吞吐量運行。HSEC許可證必須在工廠重設之前發佈，以便之後可以重複使用：

1. 重置之前：通過許可證智慧授權發佈許可證，返回本地聯機，並從智慧許可證中心刪除產品例項。
2. 重新註冊後：通過CLI手動重新應用HSEC許可證。如管理Cisco Catalyst SD-WAN中的HSEC許可證中所述，SD-WAN Manager(vManage)不支援重新安裝HSEC許可證。
3. 重新載入：在物理路由器上需要重新載入才能啟用許可證。
4. 通過`show license summary`和`show license authorization`進行驗證。

有關完整過程，請參閱在Cisco Edge路由器上配置HSECK9許可證和在Cisco Catalyst SD-WAN中管理HSEC許可證。

Q:是否可以遠端執行安全的工廠重置（通過SSH/VTY）？

A:雖然從技術角度講，此命令可以通過SSH/VTY會話發出，但強烈建議不要使用它。裝置會立即開始清理，遠端會話會被終止。重置後，裝置進入ROMMON模式，在該模式下，沒有IP連線可用，沒有可能的VTY訪問，並且需要控制檯訪問才能恢復映像。在啟動出廠重置之前，始終確保物理控制檯訪問可用。

Q:安全工廠重置是否適用於安全補救方案？

A:會。當裝置在受到可疑威脅後必須恢復為已知良好的狀態時，建議使用安全出廠重置。這可確保所有攻擊者植入的金鑰、後門或永續性機制被永久刪除，不保留任何殘留的配置或憑證資料，並確保裝置被清除以便重新登入。對於與安全相關的出廠重置，請確保在重新登入期間生成新的憑據（密碼、金鑰、證書），並且不將任何預危害備份配置還原到裝置。

Q:為什麼不改用「請求平台軟體sdwan軟體重置」或「請求平台軟體sdwan配置重置」？

A:這些命令的作用不同，並且不提供與工廠重置安全級別相同的清理級別。`request platform software sdwan software reset`命令重置SD-WAN軟體重疊，但不擦除底層Cisco IOS XE配置、金鑰、證書或儲存 — 裝置保留其基本OS狀態。`request platform software sdwan config reset`命令僅重置SD-WAN配置，但將Cisco IOS XE映像、本地憑證、SSH金鑰和磁碟上所有其他資料保持不變。這兩個命令都不會對儲存介質執行資料清理。如果目標是將裝置恢復至完全乾淨狀態（特別是在安全事件之後），則這些命令不充分，因為剩餘資料（金鑰、憑據、日誌、攻擊者植入的檔案）可能保留在快閃記憶體或SSD上。當必須保證裝置在儲存級別清潔時，請使用`factory-reset all secure`。

參考資料

- Cisco Trustworthy Systems — 出廠重置指南
- 在思科邊緣路由器上配置HSECK9許可證
- 在Cisco Catalyst SD-WAN中管理HSEC許可證
- 使用CLI生成Bootstrap檔案 — SD-WAN入門指南
- 使用vManage GUI或CLI升級SD-WAN控制器

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。