Esecuzione di un ripristino sicuro in fabbrica sui router SD-WAN cEdge

Sommario

- Introduzione
- Introduzione
- Applicabilità
- Prerequisiti
- Cosa viene cancellato
- Procedura: Secure Factory Reset
  - Passaggio 1: Accedere al dispositivo tramite console
  - Passaggio 2: Accedere alla modalità di esecuzione privilegiata
  - Passaggio 3: Eseguire il ripristino sicuro in fabbrica
  - Passaggio 4: Attendere il completamento dell'igienizzazione
  - Passaggio 5: Ripristina variabili di ambiente ROMMON
  - Passaggio 6: Avviare l'immagine software Cisco IOS XE
- Post-reimpostazione: Ricaricamento su fabric SD-WAN
- Risoluzione dei problemi
  - La console non risponde dopo il ripristino
  - Il dispositivo non entra in ROMMON
  - Variabili di ambiente mancanti in ROMMON
- Domande frequenti
- Riferimenti

Introduzione

Questo documento descrive la procedura di ripristino in fabbrica sicuro per i router di edge Cisco Catalyst SD-WAN con Cisco IOS® XE.

Introduzione

Una reimpostazione di fabbrica ripristina lo stato di produzione originale del dispositivo ed è in genere necessaria come parte dei flussi di lavoro di smantellamento, ridistribuzione o correzione della sicurezza.

⚠ Attenzione: In questo articolo viene consigliata esclusivamente l'opzione `all secure` reimpostata in `fabbrica`, che esegue la purificazione dei dati allineata con NIST SP 800-88 Rev. 1. Questo metodo rende i dati sui supporti di archiviazione irrecuperabili e fornisce il massimo livello di garanzia che i dati sensibili siano stati rimossi in modo permanente.

Applicabilità

Il comando `factory-reset all secure` è supportato sulle seguenti piattaforme con Cisco IOS XE:

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

✎ Nota: L'opzione `all secure` può essere utilizzata solo su dispositivi autonomi. Verificare che la piattaforma in uso e la versione Cisco IOS XE supporti la parola chiave `secure` selezionando `factory-reset.` in modalità di esecuzione privilegiata prima di procedere.

Prerequisiti

Prima di eseguire il ripristino sicuro in fabbrica, verificare che siano soddisfatti i seguenti prerequisiti:

- Configurazione di backup: Esportare e memorizzare in modo sicuro tutte le configurazioni, i modelli e le policy dei dispositivi da SD-WAN Manager (vManage) prima del ripristino.
- Immagini software di backup: Prima di eseguire il ripristino, accertarsi di avere una copia dell'immagine software Cisco IOS XE caricata in bootflash. Mentre l'opzione `secure` conserva l'immagine di avvio nella memoria flash sulla maggior parte delle piattaforme, alcune piattaforme eliminano completamente bootflash come parte della cancellazione sicura. In caso di emergenza, è sempre possibile avere l'immagine Cisco IOS XE disponibile su un'unità USB o su un server TFTP accessibile per garantire il ripristino indipendentemente dal comportamento della piattaforma.
- Alimentazione ininterrotta: Verificare che il dispositivo disponga di un'alimentazione ininterrotta per tutta la durata del processo di ripristino. La mancanza di corrente durante l'eliminazione può rendere il dispositivo irreversibile.

- Completare le procedure di emissione: Se sono in sospeso o in corso operazioni di aggiornamento del software in servizio (ISSU), completarle prima di avviare il ripristino in fabbrica.
- Licenza release HSEC: Prima di eseguire il ripristino in fabbrica, è necessario rilasciare la licenza HSEC dal dispositivo. Restituire la licenza HSECK9 come indicato nella sezione "Return the HSECK9 License" in: Configure HSECK9 License on Cisco Edge Router
- Rimuovi da SD-WAN Fabric: Invalidare il certificato del dispositivo da vManage e rimuovere il dispositivo dalla sovrimpressione del controller prima di eseguire la reimpostazione.
- Accesso alla console: Assicurarsi di disporre dell'accesso alla console fisica per il dispositivo. Dopo il ripristino, il dispositivo entra in modalità ROMMON e le sessioni VTY non sono disponibili.

Suggerimento: Verificare che l'immagine Cisco IOS XE sia caricata in bootflash e che una copia di ripristino sia disponibile su USB o TFTP prima di eseguire il ripristino predefinito. Mentre l'opzione `secure` conserva l'immagine di avvio sulla maggior parte delle piattaforme, alcune piattaforme purificano completamente bootflash durante il processo.

Cosa viene cancellato

Il comando `factory-reset all secure` rimuove in modo permanente questi dati dal dispositivo:

Categoria	Dati cancellati
Software	Tutte le immagini del software Cisco IOS XE (l'immagine di avvio corrente viene conservata nella memoria flash sulla maggior parte delle piattaforme; tuttavia, su alcune piattaforme bootflash è completamente purificato)
Configurazione	Configurazione di avvio, esecuzione della configurazione
Log e diagnostica	Informazioni sull'arresto anomalo, registri di sistema, OBFL (registrazione errori onboard)
Materiale di sicurezza	Chiavi e credenziali correlate a FIPS, chiavi PKI e certificati configurati dall'utente
Storage	Tutti i dati utente su storage rimovibile (SATA, SSD, USB)
Licenze	Tutte le licenze dei dispositivi (è necessaria una nuova registrazione)
ROMMON	Variabili di ambiente ROMMON aggiunte dall'utente

Nota: Questi elementi vengono mantenuti dopo il reset di fabbrica sicuro:

- Certificati SUDI (Secure Unique Device Identifier) e chiavi PKI associate
- Valore del registro di configurazione
- L'immagine d'avvio corrente (conservata nella memoria flash sulla maggior parte delle piattaforme; su alcune piattaforme, il software bootflash è completamente

---

sanificato (il ripristino USB/TFTP è sempre predisposto)

Procedura: Secure Factory Reset

Avviso: Questa procedura è irreversibile. Una volta avviati, tutti i dati elencati nella tabella precedente vengono eliminati in modo permanente. Verificare che tutti i backup siano stati verificati prima di procedere.

Passaggio 1: Accedere al dispositivo tramite console

Collegare il dispositivo tramite una connessione a una console fisica. L'accesso SSH/VTY viene perso durante il processo di ripristino.

Passaggio 2: Accedere alla modalità di esecuzione privilegiata

```
Device> enable
Device#
```

Passaggio 3: Eseguire il ripristino sicuro in fabbrica

Eseguire questo comando per avviare il ripristino sicuro in fabbrica:

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

Il sistema chiede di confermare:

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

Verifica: Alla richiesta di conferma, verificare una volta per ultima che:

- Backup di tutte le configurazioni completato
- L'immagine di ripristino di Cisco IOS XE è disponibile su USB o TFTP
- Il dispositivo è stato rimosso dalla sovrimpressione SD-WAN

Digitare `y` o premere Invio per confermare e procedere.

Passaggio 4: Attendere il completamento dell'igienizzazione

Il dispositivo esegue l'eliminazione dei dati su tutti i supporti di archiviazione. Questo processo può richiedere un periodo di tempo prolungato a seconda della capacità di storage. Non interrompere l'alimentazione durante l'operazione.

Al termine, il dispositivo si ricarica automaticamente ed entra in modalità ROMMON.

Passaggio 5: Ripristina variabili di ambiente ROMMON

Dopo il ripristino, è possibile cancellare le variabili di ambiente che includono `MAC_ADDRESS` e `SERIAL_NUMBER`. Per ripristinarli, eseguire un reset di ROMMON:

```
rommon 1> reset
```

Nota: Dopo un ripristino di fabbrica, la variabile di ambiente velocità BAUD torna al valore predefinito (9600). Se la sessione console è stata configurata a una velocità in baud diversa, è possibile regolare le impostazioni dell'emulatore di terminale a 9600 baud per recuperare l'accesso alla console.

Passaggio 6: Avviare l'immagine software Cisco IOS XE

Nella maggior parte delle piattaforme, l'opzione `secure` conserva l'immagine di avvio nella memoria flash. Verificare la presenza di `dir bootflash:` da ROMMON. Se l'immagine è disponibile, avviarla direttamente:

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

Comportamento specifico della piattaforma: Su alcune piattaforme hardware, il processo di purificazione sicura cancella completamente il bootflash, inclusa l'immagine di avvio. In questi casi, eseguire il ripristino tramite USB o TFTP.

Opzione A — Ripristino USB:

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

Opzione B — Ripristino TFTP:

Impostare le variabili di ambiente ROMMON richieste, quindi avviare il trasferimento:

```
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
```

Verificare che la connettività al server TFTP sia disponibile tramite l'interfaccia di gestione o un segmento di rete a connessione diretta. ROMMON non supporta i protocolli di routing, quindi il server TFTP deve essere raggiungibile tramite il gateway predefinito configurato.

Avere sempre un'immagine di ripristino posizionata nell'area intermedia su un server TFTP o accessibile prima di avviare il ripristino in fabbrica per tenere conto di questo comportamento.

Post-reimpostazione: Ricaricamento su fabric SD-WAN

Dopo aver ripristinato il dispositivo con un'immagine Cisco IOS XE pulita, utilizzare le procedure di onboarding SD-WAN standard per riportare il dispositivo nella struttura:

1. Configurazione bootstrap: Applicare la configurazione iniziale del bootstrap (indirizzo IP del

sistema, ID del sito, nome dell'organizzazione, indirizzo vBond). per la procedura, consultare il documento sulla generazione del file bootstrap usando la CLI.
2. Installazione certificato: Installare il certificato del dispositivo e la catena di CA radice come richiesto dall'autorità di certificazione (Symantec/DigiCert, Cisco PKI o CA dell'organizzazione).
3. Connessioni dei controlli: Verificare che siano state stabilite connessioni di controllo DTLS/TLS a vManage, vSmart e vBond.
4. Push modello: Da vManage, collegare il modello di dispositivo o il gruppo di configurazione appropriato al dispositivo.
5. Convalida: Verificare che le sessioni BFD, le route OMP e i tunnel del piano dati siano operativi.

Nota: Dopo il riavvio, la licenza HSEC (High Security) deve essere riapplicata manualmente tramite la CLI per ripristinare la velocità effettiva della crittografia. Come documentato in Gestione delle licenze HSEC in Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) non supporta la reinstallazione di una licenza HSEC su un dispositivo. Per attivare la licenza, è necessario ricaricare il dispositivo sui router fisici. Per la procedura CLI manuale, consultare il documento sulla configurazione della licenza HSECK9 sui router perimetrali Cisco.

Risoluzione dei problemi

La console non risponde dopo il ripristino

Se la console non risponde al termine del reset di fabbrica, la velocità in baud è probabilmente ripristinata ai valori predefiniti (9600). Regolare l'emulatore di terminale a 9600 baud e riconnettersi.

Il dispositivo non entra in ROMMON

Se il dispositivo non entra in ROMMON al termine del ripristino, verificare che il registro di configurazione sia impostato correttamente. Nella maggior parte dei casi, un ciclo di alimentazione forza il dispositivo in ROMMON quando non è presente alcuna immagine avviabile.

Variabili di ambiente mancanti in ROMMON

Se dopo il ripristino mancano le variabili `MAC_ADDRESS` o `SERIAL_NUMBER`, eseguire il comando `reset` in ROMMON per ripristinare le variabili di ambiente predefinite dalla memoria hardware.

Domande frequenti

Q: Perché si consiglia l'opzione "secure" rispetto alle opzioni standard "all" o "3-pass"?

A: L'opzione `factory-reset all secure` esegue la più completa purificazione dei dati disponibile, in linea con NIST SP 800-88 Rev. 1. Rende i dati irrecuperabili e mantiene l'immagine di avvio corrente in memoria flash, semplificando il ripristino. Al confronto, l'opzione `3 passaggi` esegue un pattern di sovrascrittura a tre passaggi (zero, uno, casuale) che richiede circa tre volte più tempo e cancella anche l'immagine di avvio, richiedendo un ricaricamento dell'immagine completa da USB o TFTP. L'opzione `secure` è consigliata in quanto fornisce l'eliminazione dei dati più completa con il minor sovraccarico operativo per il ripristino.

Q: Quanto tempo impiega il ripristino sicuro in fabbrica?

A: La durata varia in base alla capacità di storage totale del dispositivo. Per i dispositivi con storage flash standard (8-32 GB), il processo in genere viene completato entro 15-45 minuti. I dispositivi con storage SSD o SATA di dimensioni maggiori possono richiedere più tempo. Importante: Non interrompere l'alimentazione durante questo processo. Pianificare una finestra di manutenzione che tenga conto dei tempi di reimpostazione, ricaricamento dell'immagine e riavvio.

Q: Il dispositivo conserva la propria identità (numero di serie, SUDI) dopo il ripristino?

A: Sì. Il certificato SUDI (Secure Unique Device Identifier) e le chiavi PKI associate vengono archiviati in un archivio protetto dall'hardware (chip TAm/ACT2) e non vengono cancellati dal ripristino di fabbrica. Il numero di serie del dispositivo viene inoltre mantenuto nell'hardware. Questo significa che il dispositivo può essere riconnesso al fabric SD-WAN usando la sua identità originale dopo il reset.

Q: È necessario rimuovere il dispositivo da SD-WAN Manager prima di eseguire il ripristino?

A: Sì. Si consiglia vivamente di invalidare il certificato del dispositivo e di rimuovere il dispositivo dall'overlay SD-WAN prima di eseguire il reset di fabbrica. Ciò garantisce la rimozione dall'infrastruttura del controller, l'eliminazione delle voci obsolete nell'inventario dei dispositivi vManage e l'assenza di connessioni di controllo orfane o di stato del tunnel. Da vManage: Passare a Configurazione > Certificati > selezionare il dispositivo > Invalida, quindi Invia ai controller. Successivamente, eliminare il dispositivo dall'elenco dei dispositivi.

Q: Cosa succede alla licenza HSEC dopo il reset di fabbrica?

A: La licenza HSEC (High Security) viene rimossa durante il ripristino della fabbrica. Senza di

esso, il dispositivo funziona con un throughput di crittografia limitato. La licenza HSEC deve essere rilasciata prima del reset in fabbrica in modo da poter essere riutilizzata in seguito:

1. Prima del ripristino: Rilasciare la licenza tramite `license smart authorization, tornare alla versione locale online` e rimuovere l'istanza del prodotto da Smart License Central.
2. Dopo il riavvio: Riapplicare manualmente la licenza HSEC tramite CLI. Come documentato in Gestione delle licenze HSEC in Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) non supporta la reinstallazione della licenza HSEC.
3. Ricarica: Per attivare la licenza, è necessario ricaricare i router fisici.
4. Verificare le licenze tramite il comando `show license summary` e `show license authorization`.

Per la procedura completa, fare riferimento a Configurazione della licenza HSECK9 sui router perimetrali Cisco e Gestione delle licenze HSEC in Cisco Catalyst SD-WAN.

Q: È possibile eseguire il ripristino sicuro in fabbrica in remoto (tramite SSH/VTY)?

A: Anche se tecnicamente può essere emesso su una sessione SSH/VTY, si consiglia di farlo. Il dispositivo inizia immediatamente la purificazione e la sessione remota viene terminata. Dopo il ripristino, il dispositivo entra in modalità ROMMON (ROMMON), dove non è disponibile alcuna connettività IP, non è possibile accedere alla VTY e per il ripristino dell'immagine è necessario l'accesso alla console. Accertarsi sempre che l'accesso alla console fisica sia disponibile prima di avviare il ripristino di fabbrica.

Q: La reimpostazione di fabbrica sicura è appropriata per gli scenari di monitoraggio e aggiornamento della sicurezza?

A: Sì. Il ripristino sicuro in fabbrica è l'approccio consigliato quando un dispositivo deve essere ripristinato a uno stato riconosciuto valido dopo un presunto compromesso. Ciò garantisce che tutte le chiavi, le porte posteriori o i meccanismi di persistenza utilizzati dagli utenti malintenzionati vengano rimossi in modo permanente, che non rimangano dati di configurazione o credenziali residue e che il dispositivo sia pulito per la riaccensione. Per le reimpostazioni di fabbrica relative alla sicurezza, verificare che durante la riaccensione vengano generate nuove credenziali (password, chiavi, certificati) e che non vengano ripristinate sul dispositivo configurazioni di backup precedenti alla compromissione.

Q: Perché non utilizzare invece "request platform software sdwan software reset" o "request platform software sdwan config reset"?

A: Questi comandi hanno uno scopo diverso e non forniscono lo stesso livello di igienizzazione del `ripristino di fabbrica, il tutto protetto`. Il comando `request platform software sdwan software reset` reimposta la sovrapposizione del software SD-WAN ma non cancella le configurazioni, le chiavi, i certificati o lo storage Cisco IOS XE sottostanti. Il dispositivo conserva lo stato del sistema

operativo di base. Il comando `request platform software sdwan config reset` ripristina solo la configurazione SD-WAN, ma lascia invariate su disco l'immagine Cisco IOS XE, le credenziali locali, le chiavi SSH e tutti gli altri dati. Nessuno dei due comandi esegue l'eliminazione dei dati sul supporto di archiviazione. Se l'obiettivo è quello di riportare il dispositivo allo stato originario, in particolare dopo un incidente di sicurezza, questi comandi sono insufficienti perché i dati residui (chiavi, credenziali, registri, file piantati da utenti malintenzionati) possono rimanere nella memoria flash o nell'unità SSD. Utilizzare il `reset di fabbrica` quando è necessario garantire la pulizia del dispositivo a livello di storage.

Riferimenti

- Sistemi affidabili Cisco - Guida per il reset in fabbrica
- Configurazione della licenza HSECK9 sui router perimetrali Cisco
- Gestione delle licenze HSEC in Cisco Catalyst SD-WAN
- Generate Bootstrap File Using CLI — SD-WAN Getting Started Guide
- Aggiornamento dei controller SD-WAN con l'utilizzo di vManage GUI o CLI

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).