Réinitialisation sécurisée en usine sur les routeurs SD-WAN cEdge

Table des matières

Introduction

Ce document décrit la procédure de réinitialisation d'usine sécurisée pour les routeurs de périphérie SD-WAN Cisco Catalyst exécutant Cisco IOS® XE.

Fond

Une réinitialisation d'usine rétablit l'état de fabrication d'origine du périphérique et est généralement requise dans le cadre de workflows de mise hors service, de redéploiement ou de correction de sécurité.

⚠ Mise en garde : Cet article recommande exclusivement l'option `factory-reset all secure`, qui effectue la désinfection des données alignées sur NIST SP 800-88 Rev. 1. Cette méthode rend les données sur le support de stockage irrécupérables et fournit le plus haut niveau de garantie que les données sensibles ont été supprimées définitivement.

Applicabilité

La commande `factory-reset all secure` est prise en charge sur ces plates-formes exécutant Cisco IOS XE :

- Plates-formes de périphérie Cisco Catalyst 8200
- Plates-formes de périphérie Cisco Catalyst 8300
- Plates-formes de périphérie Cisco Catalyst 8500
- Routeurs à services d'agrégation Cisco ASR 1000
- Routeurs à services intégrés Cisco ISR 4000
- Routeurs à services intégrés Cisco ISR 1000

✎ Remarque : L'option `all secure` peut uniquement être utilisée sur des périphériques autonomes. Vérifiez que votre plate-forme et la version de Cisco IOS XE prennent en charge le mot-clé `secure` en vérifiant `factory-reset ?` en mode d'exécution privilégié avant de continuer.

Conditions préalables

Avant d'effectuer la réinitialisation sécurisée en usine, assurez-vous que les conditions suivantes sont remplies :

- Configuration de sauvegarde : Exportez et stockez en toute sécurité toutes les configurations, modèles et stratégies de périphériques à partir du gestionnaire SD-WAN (vManage) avant de les réinitialiser.
- Images logicielles de sauvegarde : Assurez-vous qu'une copie de l'image du logiciel Cisco IOS XE est chargée dans la mémoire flash de démarrage avant d'effectuer la réinitialisation. Alors que l'option `secure` conserve l'image de démarrage en mémoire flash sur la plupart des plates-formes, certaines plates-formes désinfectent entièrement bootflash dans le cadre de la suppression sécurisée. En cas d'urgence, assurez-vous que l'image Cisco IOS XE est toujours disponible sur un lecteur USB ou un serveur TFTP accessible pour garantir la récupération, quel que soit le comportement de la plate-forme.

- Alimentation ininterrompue : Assurez-vous que le périphérique dispose d'une alimentation ininterrompue tout au long du processus de réinitialisation. Une perte d'alimentation lors de la désinfection peut rendre le périphérique irrécupérable.
- Suivez toutes les procédures ISSU : Si des opérations ISSU (In-Service Software Upgrade) sont en attente ou en cours, terminez-les avant de lancer la réinitialisation en usine.
- Libérer la licence HSEC : La licence HSEC doit être libérée du périphérique avant d'effectuer la réinitialisation en usine. Retournez la licence HSECK9 comme indiqué dans la section « Retourner la licence HSECK9 » à l'adresse : Configurer la licence HSECK9 sur les routeurs de périphérie Cisco
- Supprimer de la matrice SD-WAN : Invalidez le certificat du périphérique à partir de vManage et supprimez le périphérique de la superposition du contrôleur avant d'effectuer la réinitialisation.
- Accès console : Assurez-vous que vous disposez d'un accès physique à la console du périphérique. Après la réinitialisation, le périphérique passe en mode ROMMON et les sessions VTY ne sont pas disponibles.

Conseil : Vérifiez que l'image Cisco IOS XE est chargée dans le bootflash et qu'une copie de récupération est disponible sur USB ou TFTP avant d'exécuter la réinitialisation d'usine. Alors que l'option `secure` conserve l'image de démarrage sur la plupart des plates-formes, certaines plates-formes désinfectent complètement bootflash pendant le processus.

Ce qui est supprimé

La commande `factory-reset all secure` supprime définitivement ces données du périphérique :

Catégorie	Données effacées
le logiciel Cisco IOS	Toutes les images du logiciel Cisco IOS XE (l'image de démarrage actuelle est conservée dans la mémoire flash sur la plupart des plates-formes ; cependant, sur certaines plates-formes, bootflash est entièrement nettoyé)
Configuration	Configuration initiale, configuration en cours
Journaux et diagnostics	Informations sur les pannes, journaux système, OBFL (consignation des pannes internes)
Matériel De Sécurité	Clés et informations d'identification FIPS, clés PKI configurées par l'utilisateur et certificats
Stockage	Toutes les données utilisateur sur le stockage amovible (SATA, SSD, USB)
Licences	Toutes les licences de périphérique (réenregistrement requis)
ROMMON	Variables d'environnement ROMMON ajoutées par l'utilisateur

---

Remarque : Ces éléments sont conservés après la réinitialisation d'usine sécurisée :

- Certificats SUDI (Secure Unique Device Identifier) et clés PKI associées
- Valeur du registre de configuration
- L'image de démarrage actuelle (conservée dans la mémoire flash sur la plupart des plates-formes ; sur certaines plates-formes, le bootflash est entièrement nettoyé ; assurez-vous que la récupération USB/TFTP est toujours effectuée)

Procédure: Réinitialisation sécurisée en usine

Avertissement : Cette procédure est irréversible. Une fois initiées, toutes les données répertoriées dans le tableau précédent sont définitivement détruites. Assurez-vous que toutes les sauvegardes ont été vérifiées avant de continuer.

Étape 1: Accès au périphérique via la console

Se connecter au périphérique via une connexion de console physique. L'accès SSH/VTY est perdu pendant le processus de réinitialisation.

Étape 2: Passez en mode privilégié

```
Device> enable
Device#
```

Étape 3: Exécuter la réinitialisation sécurisée en usine

Exécutez cette commande pour lancer la réinitialisation d'usine sécurisée :

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

Le système vous invite à confirmer :

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

⚠ Vérifier : À l'invite de confirmation, vérifiez une dernière fois que :

- Toutes les configurations ont été sauvegardées
- L'image de récupération de Cisco IOS XE est disponible sur USB ou TFTP
- Le périphérique a été supprimé de la superposition SD-WAN

Tapez `y` ou appuyez sur Entrée pour confirmer et continuer.

Étape 4: Attendre la fin de l'assainissement

Le périphérique procède à la désinfection des données sur tous les supports de stockage. Ce processus peut prendre une période prolongée en fonction de la capacité de stockage. N'interrompez pas l'alimentation pendant cette opération.

Une fois terminé, le périphérique se recharge automatiquement et passe en mode ROMMON.

Étape 5: Restaurer les variables d'environnement ROMMON

Après la réinitialisation, les variables d'environnement, y compris `MAC_ADDRESS` et `SERIAL_NUMBER`, peuvent être effacées. Effectuez une réinitialisation ROMMON pour les restaurer :

```
rommon 1> reset
```

✎ Remarque : La variable d'environnement de taux BAUD revient à sa valeur par défaut (9600) après une réinitialisation d'usine. Si votre session en mode console a été configurée avec un débit en bauds différent, vous pouvez régler les paramètres de l'émulateur de terminal sur 9 600 bauds pour rétablir l'accès à la console.

Étape 6: Démarrer l'image du logiciel Cisco IOS XE

Sur la plupart des plates-formes, l'option `secure` conserve l'image de démarrage dans la mémoire flash. Vérifiez sa présence avec `dir bootflash:` de ROMMON. Si l'image est disponible, démarrez directement :

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

Comportement spécifique à la plate-forme : Sur certaines plates-formes matérielles, le processus de désinfection sécurisé efface entièrement bootflash, y compris l'image de démarrage. Dans ce cas, récupérez via USB ou TFTP.

Option A — Récupération USB :

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

Option B : récupération TFTP :

Définissez les variables d'environnement ROMMON requises, puis lancez le transfert :

```
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
```

Vérifiez que la connectivité au serveur TFTP est disponible via l'interface de gestion ou un segment de réseau directement connecté. ROMMON ne prenant pas en charge les protocoles de routage, le serveur TFTP doit être accessible via la passerelle par défaut configurée.

Veillez à toujours préparer une image de récupération sur USB ou un serveur TFTP accessible avant de lancer la réinitialisation d'usine pour prendre en compte ce comportement.

Après la réinitialisation : Réintégration à la structure SD-WAN

Une fois que le périphérique a été restauré avec une image propre de Cisco IOS XE, utilisez les procédures d'intégration SD-WAN standard pour ramener le périphérique dans le fabric :

1. Configuration du bootstrap : Appliquez la configuration initiale des données d'amorçage (IP système, ID de site, nom d'organisation, adresse vBond). Référez-vous à Générer un fichier d'amorçage à l'aide de CLI pour la procédure.
2. Installation du certificat : Installez le certificat du périphérique et la chaîne de l'autorité de certification racine, comme requis par votre autorité de certification (Symantec/DigiCert, Cisco PKI ou Enterprise CA).
3. Connexions de contrôle : Vérifiez que les connexions de contrôle DTLS/TLS sont établies avec vManage, vSmart et vBond.
4. Diffusion du modèle : À partir de vManage, associez le modèle de périphérique ou le groupe de configuration approprié au périphérique.
5. Validation : Vérifiez que les sessions BFD, les routes OMP et les tunnels du plan de données sont opérationnels.

Remarque : Après la réintégration, la licence HSEC (High Security) doit être réappliquée manuellement via l'interface de ligne de commande pour restaurer le débit de cryptage. Comme l'explique la section Gestion des licences HSEC dans Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) ne prend pas en charge la réinstallation d'une licence HSEC sur un périphérique. Un rechargement de périphérique est nécessaire sur les routeurs physiques pour activer la licence. Référez-vous à Configurer la licence HSECK9 sur les routeurs de périphérie Cisco pour la procédure de CLI manuelle.

Dépannage

La console ne répond pas après la réinitialisation

Si la console ne répond pas une fois la réinitialisation d'usine terminée, le débit en bauds est probablement revenu à la valeur par défaut (9600). Réglez l'émulateur de terminal sur 9 600 bauds et reconnectez-vous.

Le périphérique n'entre pas dans ROMMON

Si le périphérique n'entre pas dans ROMMON une fois la réinitialisation terminée, vérifiez que le registre de configuration est correctement défini. Dans la plupart des cas, un cycle d'alimentation force le périphérique à entrer en mode ROMMON lorsqu'aucune image de démarrage n'est présente.

Variables d'environnement manquantes dans ROMMON

Si des variables `MAC_ADDRESS` ou `SERIAL_NUMBER` sont manquantes après la réinitialisation, émettez la commande `reset` dans ROMMON pour restaurer les variables d'environnement par défaut d'usine à partir du stockage matériel.

Foire aux questions

Q : Pourquoi l'option « secure » est-elle recommandée par rapport aux options standard « all » ou « 3-pass » ?

A : L'option `factory-reset all secure` effectue la désinfection des données la plus complète disponible, alignée sur NIST SP 800-88 Rev. 1. Elle rend les données irrécupérables et conserve l'image de démarrage actuelle en mémoire flash, ce qui simplifie la récupération. Par comparaison, l'option `3 passes` effectue un modèle d'écrasement à trois passes (zéros, uns, aléatoires) qui prend environ trois fois plus de temps et efface également l'image de démarrage, nécessitant un rechargement complet de l'image à partir d'USB ou TFTP. L'option `secure` est recommandée car elle fournit la désinfection la plus complète avec le moins de surcharge opérationnelle pour la récupération.

Q : Combien de temps dure la réinitialisation d'usine sécurisée ?

A : La durée varie en fonction de la capacité de stockage totale du périphérique. Pour les périphériques avec stockage Flash standard (8-32 Go), le processus se termine généralement en 15-45 minutes. Les périphériques disposant d'un stockage SSD ou SATA plus important peuvent prendre plus de temps. Important : N'interrompez pas l'alimentation pendant ce processus. Planifiez une fenêtre de maintenance qui tient compte de la réinitialisation, du rechargement de l'image et du temps de réintégration.

Q : Le périphérique conserve-t-il son identité (numéro de série, SUDI) après la réinitialisation ?

A : Oui. Le certificat Secure Unique Device Identifier (SUDI) et ses clés PKI associées sont stockés dans une mémoire protégée par matériel (puce TAm/ACT2) et ne sont pas effacés par la réinitialisation en usine. Le numéro de série du périphérique est également conservé dans le matériel. Cela signifie que le périphérique peut être réintégré dans le fabric SD-WAN en utilisant son identité d'origine après la réinitialisation.

Q : Dois-je retirer le périphérique du Gestionnaire SD-WAN avant d'effectuer la réinitialisation ?

A : Oui. Il est fortement recommandé d'invalider le certificat du périphérique et de le retirer de la superposition SD-WAN avant d'effectuer la réinitialisation d'usine. Cela garantit une suppression nette de l'infrastructure du contrôleur, l'absence d'entrées périmées dans l'inventaire des périphériques vManage et l'absence de connexions de contrôle orphelines ou d'état de tunnel. À

partir de vManage : Accédez à Configuration > Certificates > sélectionnez le périphérique > Invalidate, puis Send to Controllers. Ensuite, supprimez le périphérique de la liste des périphériques.

Q : Qu'advient-il de la licence HSEC après la réinitialisation en usine ?

A : La licence HSEC (High Security) est supprimée lors de la réinitialisation en usine. Sans cela, le périphérique fonctionne avec un débit de cryptage restreint. La licence HSEC doit être libérée avant la réinitialisation d'usine afin de pouvoir être réutilisée par la suite :

1. Avant la réinitialisation : Libérez la licence via le `retour d'autorisation Smart de licence local en ligne` et supprimez l'instance de produit de Smart License Central.
2. Après réintégration : Réappliquez manuellement la licence HSEC via l'interface de ligne de commande. Comme l'indique la section Gestion des licences HSEC dans Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) ne prend pas en charge la réinstallation de la licence HSEC.
3. Recharger : Un rechargement est nécessaire sur les routeurs physiques pour activer la licence.
4. Vérifiez via `show license summary` et `show license authorization`.

Pour la procédure complète, référez-vous à Configurer la licence HSECK9 sur les routeurs de périphérie Cisco et à Gérer les licences HSEC dans Cisco Catalyst SD-WAN.

Q : Puis-je effectuer la réinitialisation d'usine sécurisée à distance (via SSH/VTY) ?

A : Bien que la commande puisse techniquement être émise sur une session SSH/VTY, elle est fortement déconseillée. Le périphérique commence immédiatement la désinfection et la session distante est interrompue. Après la réinitialisation, le périphérique passe en mode ROMMON où aucune connectivité IP n'est disponible, aucun accès VTY n'est possible et un accès console est requis pour la récupération d'image. Assurez-vous toujours que l'accès à la console physique est disponible avant de lancer la réinitialisation d'usine.

Q : La réinitialisation d'usine sécurisée est-elle appropriée pour les scénarios de correction de sécurité ?

A : Oui. La réinitialisation sécurisée en usine est l'approche recommandée lorsqu'un périphérique doit être remis dans un état de fonctionnement normal après une compromission suspectée. Cela garantit que toutes les clés, portes dérobées ou mécanismes de persistance installés par le pirate sont définitivement supprimés, qu'aucune configuration résiduelle ou donnée d'identification ne reste et que le périphérique est nettoyé pour être réintégré. Pour les réinitialisations d'usine liées à la sécurité, assurez-vous que de nouvelles informations d'identification (mots de passe, clés, certificats) sont générées lors de la réintégration et qu'aucune configuration de sauvegarde

préalable à la compromission n'est restaurée sur le périphérique.

Q : Pourquoi ne pas utiliser « request platform software sdwan software reset » ou « request platform software sdwan config reset » ?

A : Ces commandes ont un objectif différent et ne fournissent pas le même niveau de désinfection que `factory-reset all secure`. La commande `request platform software sdwan software reset` réinitialise la superposition du logiciel SD-WAN mais n'efface pas les configurations, clés, certificats ou stockage sous-jacents de Cisco IOS XE — le périphérique conserve son état de système d'exploitation de base. La commande `request platform software sdwan config reset` réinitialise uniquement la configuration SD-WAN mais laisse intacts sur le disque l'image Cisco IOS XE, les informations d'identification locales, les clés SSH et toutes les autres données. Aucune de ces commandes ne procède à la désinfection des données sur le support de stockage. Si l'objectif est de remettre le périphérique dans un état entièrement propre, en particulier après un incident de sécurité, ces commandes sont insuffisantes car les données résiduelles (clés, informations d'identification, journaux, fichiers placés par le pirate) peuvent rester sur la mémoire flash ou le disque SSD. Utilisez `factory-reset all secure` quand le périphérique doit être garanti propre au niveau de stockage.

Références

- Cisco Trustworthy Systems - Guide de réinitialisation en usine
- Configuration de la licence HSECK9 sur les routeurs de périphérie Cisco
- Gestion des licences HSEC dans Cisco Catalyst SD-WAN
- Générer un fichier d'amorçage à l'aide de CLI - Guide de démarrage SD-WAN
- Mise à niveau des contrôleurs SD-WAN à l'aide de l'interface utilisateur graphique ou CLI vManage

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.