SD-WAN cEdgeルータでの工場出荷時安全リセットの実行

内容

はじめに

このドキュメントでは、Cisco IOS® XEを実行するCisco Catalyst SD-WANエッジルータの工場での安全なリセット手順について説明します。

背景

工場出荷時の状態にリセットすると、デバイスは元の製造状態に戻ります。通常は、使用停止、再導入、またはセキュリティ修復のワークフローの一部として必要です。

⚠

注意：この記事では、NIST SP 800-88 Rev. 1に従ってデータのサニタイズを実行する `factory-reset all secure`オプションのみを推奨しています。この方法では、ストレージメディア上のデータが回復不能になり、機密データが完全に削除されたことを保証します。

適用性

`factory-reset all secure`コマンドは、Cisco IOS XEを実行する次のプラットフォームでサポートされています。

- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cisco ISR 4000シリーズサービス統合型ルータ
- Cisco ISR 1000シリーズサービス統合型ルータ

注：`all secure`オプションは、スタンドアロンデバイスでのみ使用できます。先に進む前に、特権EXECモードで`factory-reset ?`をチェックして、プラットフォームとCisco IOS XEバージョンが`secure`キーワードをサポートしていることを確認します。

前提条件

セキュアな工場出荷時設定へのリセットを実行する前に、次の前提条件が満たされていることを確認します。

- バックアップ設定：リセットする前に、SD-WAN Manager(vManage)からすべてのデバイス設定、テンプレート、およびポリシーをエクスポートして安全に保存します。
- バックアップソフトウェアイメージ：リセットを実行する前に、ブートフラッシュにロードされたCisco IOS XEソフトウェアイメージのコピーがあることを確認してください。`secure`オプションを使用すると、ほとんどのプラットフォームでブートイメージがフラッシュ内に保持されますが、特定のプラットフォームでは、ブートフラッシュ全体がセキュアワイプの一部としてサニタイズされます。プラットフォームの動作に関係なくリカバリを保証するために、Cisco IOS XEイメージを常にUSBドライブまたはアクセス可能なTFTPサーバで使用できるようにしてください。
- 無停電電源：リセットプロセス全体を通して、デバイスに無停電電源が供給されていることを確認します。サニタイズ中の電力損失により、デバイスが回復不能になる可能性があります。

- ISSUの手順をすべて実行します。In-Service Software Upgrade(ISSU)操作が保留中または進行中の場合は、工場出荷時設定へのリセットを開始する前に操作を実行します。
- HSECライセンスのリリース：HSECライセンスは、工場出荷時設定に戻す前にデバイスからリリースする必要があります。 「HSECK9ライセンスの返却」の項(「Ciscoエッジルータでの HSECK9ライセンスの設定」)の説明に従って、HSECK9ライセンスを返却します。
- SD-WANファブリックから削除：vManageからデバイス証明書を無効にし、コントローラオーバーレイからデバイスを削除してから、リセットを実行します。
- コンソールアクセス：デバイスへの物理的なコンソールアクセスがあることを確認します。リセット後、デバイスはROMMONモードになり、VTYセッションは使用できません。

ヒント:Cisco IOS XEイメージがブートフラッシュにロードされていること、および工場出荷時設定へのリセットを実行する前に、USBまたはTFTPで回復コピーが使用可能であることを確認します。`secure`オプションを使用すると、ほとんどのプラットフォームでブートイメージが保持されますが、一部のプラットフォームでは、処理中にブートフラッシュのイメージが完全に消去されます。

消去対象

`factory-reset all secure`コマンドは、デバイスから次のデータを永久に削除します。

[Category]	データの消去
[ソフトウェア（Software）]	すべてのCisco IOS XEソフトウェアイメージ（現在のブートイメージはほとんどのプラットフォームのフラッシュに保持されますが、特定のプラットフォームではブートフラッシュの内容が完全に消去されます）
コンフィギュレーション	スタートアップコンフィギュレーション、実行コンフィギュレーション
ログと診断	クラッシュ情報、システムログ、OBFL（オンボード障害ロギング）
セキュリティ資料	FIPS関連のキーとクレデンシャル、ユーザ設定のPKIキーと証明書
ストレージ	リムーバブルストレージ(SATA、SSD、USB)上のすべてのユーザデータ
ライセンス	すべてのデバイスライセンス（再登録が必要）
ロード	ユーザが追加したROMMON環境変数

注：次の項目は、セキュアな工場出荷時設定にリセットした後も保持されます。

- SUDI(Secure Unique Device Identifier)証明書および関連するPKIキー
- コンフィギュレーションレジスタ値
- 現在のブートイメージ（ほとんどのプラットフォームのフラッシュに保持され、特定のプラットフォームではブートフラッシュは完全にサニタイズされ、常にUSB/TFTPリカバリがステージングされる）

手順：工場出荷時状態への安全なリセット

警告：この手順は元に戻せません。いったん開始すると、前の表にリストされているすべてのデータは完全に破棄されます。続行する前に、すべてのバックアップが確認されていることを確認してください。

ステップ1：コンソール経由でデバイスにアクセスする

物理的なコンソール接続を介してデバイスに接続します。リセットプロセス中にSSH/VTYアクセスが失われる。

ステップ2：特権EXECモードに入る

```
Device> enable
Device#
```

ステップ3：セキュアファクトリリセットの実行

次のコマンドを実行して、セキュアな工場出荷時設定へのリセットを開始します。

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

確認を求めるプロンプトが表示されます。

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

Check：確認プロンプトで、次の内容を確認します。

- すべての構成がバックアップされました
- Cisco IOS XEリカバリイメージは、USBまたはTFTPで使用できます
- デバイスはSD-WANオーバーレイから削除されました

yと入力するかEnterキーを押して確定し、続行します。

ステップ4：サニタイズが完了するのを待つ

デバイスは、すべてのストレージメディアでデータのサニタイズを実行します。ストレージ容量によっては、このプロセスに長時間かかる場合があります。この操作中は電源を遮断しないでください。

完了すると、デバイスは自動的にリロードされ、ROMMONモードに入ります。

ステップ5:ROMMON環境変数の復元

リセット後に、MAC_ADDRESSおよびSERIAL_NUMBERを含む環境変数をクリアできます。ROMMONのリセットを実行して、これらを復元します。

```
rommon 1> reset
```

注:BAUD rate環境変数は、工場出荷時設定に戻すとデフォルト値(9600)に戻ります。コンソールセッションが異なるボーレートで設定されている場合は、ターミナルエミュレータの設定を9600ボーに調整して、コンソールアクセスを回復できます。

ステップ6:Cisco IOS XEソフトウェアイメージを起動する

ほとんどのプラットフォームでは、secureオプションを使用するとブートイメージをフラッシュ内に保持できます。ROMMONからdir bootflash:を使用して、存在を確認します。イメージが使用可能な場合は、直接ブートします。

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

プラットフォーム固有の動作：特定のハードウェアプラットフォームでは、セキュアなサニタイズ処理により、ブートイメージを含むブートフラッシュ全体が消去されます。このような場合は、USBまたはTFTPを使用して回復します。

選択肢A — USBリカバリ：

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

選択肢B — TFTPリカバリ：

必要なROMMON環境変数を設定してから、転送を開始します。

```
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
```

管理インターフェイスまたは直接接続されたネットワークセグメントを介してTFTPサーバへの接続が可能であることを確認します。ROMMONではルーティングプロトコルがサポートされていないため、設定されたデフォルトゲートウェイを介してTFTPサーバに到達できる必要があります。

この動作に対処するために工場出荷時状態へのリセットを開始する前に、USB またはアクセス可能なTFTPサーバにリカバリイメージをステージングしておいてください。

リセット後：SD-WANファブリックへの再オンボーディング

デバイスがクリーンなCisco IOS XEイメージで復元されたら、標準のSD-WANオンボーディング手順を使用して、デバイスをファブリックに戻します。

1. ブートストラップ設定：初期ブートストラップ設定（システムIP、サイトID、組織名、vBondアドレス）を適用します。 手順については、『CLIを使用したブートストラップファイルの生成』を参照してください。
2. 証明書のインストール：認証局（Symantec/DigiCert、Cisco PKI、またはエンタープライズ

CA）の要求に応じて、デバイス証明書およびルートCAチェーンをインストールします。
3. 制御接続：vManage、vSmart、およびvBondに対してDTLS/TLS制御接続が確立されていることを確認します。
4. テンプレートプッシュ：vManageから、適切なデバイステンプレートまたは設定グループをデバイスに接続します。
5. 検証：BFDセッション、OMPルート、およびデータプレーントンネルが動作可能であることを確認します。

注：再オンボーディング後、暗号化スループットを復元するには、HSEC(High Security)ライセンスをCLIから手動で再適用する必要があります。「Cisco Catalyst SD-WANでのHSECライセンスの管理」に記載されているように、SD-WAN Manager(vManage)では、デバイスへのHSECライセンスの再インストールはサポートされていません。ライセンスをアクティブにするには、物理ルータでデバイスのリロードが必要です。手動CLI手順については、「CiscoエッジルータでのHSECK9ライセンスの設定」を参照してください。

トラブルシューティング

リセット後にコンソールが応答しない

初期設定へのリセットが完了した後、コンソールが応答しない場合は、ボーレートがデフォルト(9600)に戻っている可能性があります。 ターミナルエミュレータを9600ボーに調整し、再接続します。

デバイスがROMMONにならない

リセットが完了してもデバイスがROMMONにならない場合は、コンフィギュレーションレジスタが正しく設定されていることを確認します。ほとんどの場合、ブート可能なイメージが存在しないときは、電源の再投入によってデバイスが強制的にROMMON状態になります。

ROMMONで環境変数が見つからない

リセット後に`MAC_ADDRESS`または`SERIAL_NUMBER`変数が失われた場合、ROMMONで`reset`コマンドを発行して、ハードウェアストレージから工場出荷時のデフォルトの環境変数を復元します。

FAQ

Q：標準の「すべて」または「3パス」オプションに対して、「セキュア」オプションが推奨されるのはなぜですか。

A:factory-reset all secureオプションでは、NIST SP 800-88 Rev. 1に従って、利用可能な最も詳細なデータサニタイズが実行されます。データをリカバリ不能にし、現在のブートイメージをフラッシュに保持するため、リカバリが容易になります。一方、3-passオプションでは3パス上書きパターン（ゼロ、1、ランダム）が実行されます。このパターンでは約3倍の時間がかかり、ブートイメージも消去されるため、USBまたはTFTPからイメージを完全にリロードする必要があります。secureオプションを使用することを推奨いたします。このオプションでは、リカバリの運用オーバーヘッドを最小限に抑えながら、最も詳細なサニタイズを実現できます。

Q：工場出荷時状態への安全なリセットにはどれくらいの時間がかかりますか。

A：期間は、デバイスのストレージ容量の合計によって異なります。標準のフラッシュストレージ(8 ~ 32 GB)を備えたデバイスの場合、このプロセスは通常15 ~ 45分以内に完了します。SSDまたはSATAストレージの容量が大きいデバイスは、時間がかかる可能性があります。重要：この処理中に電源を遮断しないでください。リセットとイメージのリロードおよび再オンボーディングの時間を考慮したメンテナンス期間を計画します。

Q：リセット後もデバイスのID（シリアル番号、SUDI）は保持されますか。

A:はい。Secure Unique Device Identifier(SUDI)証明書とそれに関連するPKIキーは、ハードウェアで保護されたストレージ（TAm/ACT2チップ）に保存され、工場出荷時のリセットでは消去されません。デバイスのシリアル番号もハードウェアに保存されます。つまり、リセット後に元のIDを使用して、デバイスをSD-WANファブリックに再オンボーディングできます。

Q：リセットを実行する前に、SD-WAN Managerからデバイスを削除する必要がありますか。

A:はい。デバイスの証明書を無効にし、工場出荷時のリセットを実行する前に、SD-WANオーバーレイからデバイスを削除することを強くお勧めします。これにより、コントローラインフラストラクチャからのクリーンな削除、vManageデバイスインベントリ内の古いエントリの排除、孤立したコントロール接続やトンネル状態の排除が可能になります。vManageから、Configuration > Certificatesの順に移動し、デバイスを選択> Invalidateの後、Send to Controllersの順に選択します。その後、デバイスリストからデバイスを削除します。

Q：工場出荷時設定にリセットした後、HSECライセンスはどうなりますか。

A:HSEC(High Security)ライセンスは、工場出荷時のリセット時に削除されます。これを使用しない場合、デバイスは制限された暗号化スループットで動作します。HSECライセンスは、工場出荷時設定に戻す前にリリースし、後で再利用できるようにする必要があります。

1. リセットする前に：ライセンススマート認証でローカルオンラインに戻ってライセンスをリリースし、Smart License Centralから製品インスタンスを削除します。
2. 再オンボーディング後：CLIを使用してHSECライセンスを手動で再適用します。「Cisco Catalyst SD-WANでのHSECライセンスの管理」に記載されているように、SD-WAN Manager(vManage)ではHSECライセンスの再インストールはサポートされていません。
3. リロード：ライセンスをアクティブにするには、物理ルータのリロードが必要です。
4. `show license summary`および`show license authorization`を使用して確認します。

完全な手順については、「CiscoエッジルータでのHSECK9ライセンスの設定」および「Cisco Catalyst SD-WANでのHSECライセンスの管理」を参照してください。

Q：工場出荷時の安全なリセットを（SSH/VTY経由で）リモートで実行できますか。

A：このコマンドはSSH/VTYセッション経由で技術的に発行できますが、強く推奨しません。デバイスはすぐにサニタイズを開始し、リモートセッションが終了します。リセット後、デバイスはROMMONモードに入ります。このモードでは、IP接続は使用できず、VTYアクセスは不可能です。また、イメージの回復にはコンソールアクセスが必要です。工場出荷時設定へのリセットを開始する前に、必ず物理的なコンソールアクセスが利用可能であることを確認してください。

Q：工場出荷時の安全なリセットは、セキュリティ修復シナリオに適していますか。

A:はい。安全な工場出荷時状態へのリセットは、侵害が疑われる状況でデバイスを正常な状態に戻す必要がある場合に推奨されるアプローチです。これにより、攻撃者が仕掛けたキー、バックドア、または持続性メカニズムがすべて完全に削除され、設定やクレデンシャルデータが残存することがなくなり、デバイスが再オンボーディング用にクリーンであることが保証されます。セキュリティ関連の工場出荷時設定のリセットに関しては、新しいクレデンシャル（パスワード、キー、証明書）が再オンボーディング時に生成され、妥協のないバックアップ設定がデバイスに復元されることを確認してください。

Q：代わりに「request platform software sdwan software reset」または「request platform software sdwan config reset」を使用してください。

A：これらのコマンドは異なる目的で使用され、`factory-reset all secure`と同じレベルのサニタイズは提供しません。`request platform software sdwan software reset`コマンドは、SD-WANソフトウェアオーバーレイをリセットしますが、基盤となるCisco IOS XE構成、鍵、証明書、またはストレージを消去しません。デバイスは基本OSの状態を保持します。`request platform software sdwan config reset`コマンドは、SD-WAN設定のみをリセットしますが、Cisco IOS XEイメージ、ローカルクレデンシャル、SSHキー、およびその他すべてのデータはディスク上でそのまま保持されます。どちらのコマンドも、ストレージメディア上でデータのサニタイズを実行しません。デバイスを完全にクリーンな状態に戻すことが目的の場合、特にセキュリティインシデント後には、これらのコマンドは不十分です。これは、残存データ（キー、クレデンシャル、ログ、攻撃者が仕掛けたファイル）がフラッシュまたはSSDに残る可能性があるためです。デバイスがスト

レージレベルでクリーンであることが保証される必要がある場合は、`factory-reset all secure`を使用します。

参照資料

- Cisco Trustworthy Systems – 工場出荷時設定へのリセットガイド
- CiscoエッジルータでのHSECK9ライセンスの設定
- Cisco Catalyst SD-WANでのHSECライセンスの管理
- CLIを使用したブートストラップファイルの生成 – SD-WAN入門ガイド
- vManage GUIまたはCLIを使用したSD-WANコントローラのアップグレード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。