Dell EMC SmartFabric OS10 セキュリティ ベスト プラクティス ガイド

2021 年 5 月

5 月 2021 年
Rev. A05

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: **ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。**

警告: **物的損害、けが、または死亡の原因となる可能性があることを示しています。**

©2020 年 ~ 2021 年 Dell Inc.またはその関連会社。All rights reserved. (不許複製・禁無断転載) Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

目次

1

OS10 セキュリティのベスト プラクティス

このドキュメントでは、Dell EMC SmartFabric OS10 を実行するスイッチを保護するための推奨事項をまとめています。詳細な構成については、『*Dell EMC SmartFabric OS10 ユーザー ガイド*』を参照してください。

Dell EMC のドキュメントは、https://www.dell.com/support/で入手できます。

[適用性]

このドキュメントに記載されている推奨事項は、Dell EMC SmartFabric OS10.5.x.x に適用されます。

最初の起動時

初めてスイッチを起動すると、システムはゼロタッチ導入（ZTD）を実行します。ZTD は OS10 イメージのアップグレードを自動化し、CLI バッチ ファイルを実行してスイッチを構成し、ZTD 後のスクリプトを実行して追加の機能を実行します。システムでは、ZTD はデフォルトで有効になっています。ZTD を使用しない場合は、`ztd cancel` コマンドを使用して ZTD を無効にできます。OS10 に最初にログインした後、デフォルトのパスワードを変更して OS10 を最新バージョンにアップグレードします。これには、新機能とセキュリティの修正が含まれている場合があります。

[デフォルト CLI パスワードの変更]

[論拠]: 初めてスイッチにログ インすると、システムによりユーザー名の入力を求めるプロンプトが表示され、コマンドライン インターフェイスが起動します。初めて OS10 にログ インするには、ユーザー名（`admin`）とパスワードを入力します。安全なところに最初にログインした後にデフォルトの `admin` パスワードを変更するか、`sysadmin` の役割を持つ OS10 ユーザーを少なくとも 1 人作成して、デフォルトの `admin` ユーザー名を削除します。システムにより、今後のログインのために新しいパスワードが保存されます。CLI を使用してパスワードを変更した後、`write memory` コマンドを使用して構成を保存します。

[構成]:

```
OS10# configure terminal
% Error: ZTD is in progress(configuration is locked).
OS10# ztd cancel
OS10# configure terminal
OS10(config)# username admin password new-password role sysadmin
OS10(config)# exit
OS10# write memory
```

デフォルトの `admin` ユーザー名を削除するには、`sysadmin` ロールを持つ異なるアカウントにログ インし、次の手順を実行します。

```
OS10(config)# no username admin
```

システムに構成されたすべてのユーザーの詳細を表示するには、次のコマンドを使用します。

```
OS10# show running-configuration users
```

[デフォルトの linuxadmin パスワードの変更]

[論拠]: トラブルシューティングおよび診断目的では、Linux シェルを使用します。OS10 に最初にログインした後、デフォルトの Linux シェルのユーザー名とパスワードの両方に `linuxadmin` を入力し、デフォルトの `linuxadmin` パスワードを変更します。システムにより、今後のログインのために新しいパスワードが保存されます。CLI を使用してパスワードを変更した後、`write memory` コマンドを使用して構成を保存します。

[構成]:

```
OS10# configure terminal
OS10(config)# system-user linuxadmin password {clear-text-password | hashed-password}
OS10(config)# exit
OS10# write memory
```

[linuxadmin アカウントの無効化]

[論拠]: ユーザーに Linux シェルへのアクセスを許可しない場合は、`linuxadmin` アカウントを無効にします。

[構成]:

```
OS10(config)# system-user linuxadmin disable
OS10(config)# exit
OS10# write memory
```

[Linux コマンドへのアクセスの無効化]

[論拠]: `linuxadmin` ユーザーを無効化した場合でも、ユーザーは `system` コマンドを使用して Linux コマンドにアクセスできます。Linux コマンドへのアクセスを完全に無効にするには、`system-cli` コマンドを使用します。

[構成]:

```
OS10(config)# system-cli disable
OS10(config)# exit
OS10# write memory
```

[使用していないインターフェイスの無効化]

[論拠]: 不正ユーザーがフロントエンド インターフェイス上のネットワークに接続できないようにするには、使用していないインターフェイスを無効にします。

[構成]:

```
OS10(config)# interface range ethernet 1/1/10-1/1/32
OS10(conf-range-eth1/1/10-1/1/32)# shutdown
OS10(conf-range-eth1/1/10-1/1/32)# end
OS10# write memory
```

[ブートローダー保護の有効化]

[論拠]: 悪意のある不正ユーザーがスイッチにアクセスできないようにするには、GRUB パスワードを使用してブートローダーを保護します。

[構成]:

```
OS10# boot protect enable username username password password
OS10# write memory
```

[ブートローダーの保護が有効になっているかどうかのチェック]

次のコマンドを使用して、システムのブートローダー保護のステータスを表示します。

```
OS10# show boot protect
Boot protection enabled
Authorized users: root linuxadmin admin
```

パスワード ルール

厳格なパスワード ルールにより、デバイスのセキュリティを向上させることができます。

[強力なパスワードの有効化]

[論拠]: 強力なパスワードを使用すれば、推測することは非常に困難になります。デフォルトでは、強力なパスワードのチェックがシステムで有効になっており、パスワードに英数字と特殊文字が含まれているかどうかをチェックできます。強力なパスワードのチェックが無効になっている場合は、有効にします。

[構成]:

```
OS10(config)# no service simple-password
OS10(config)# exit
OS10# write memory
```

[強力なパスワードのチェックが有効になっているかどうかのチェック]

デフォルトでは、強力なパスワードのチェックはシステムで有効化されており、`no service simple-password` コマンドは実行中の構成で黙示的になっています。強力なパスワードのチェックを有効にしているかどうかを確認するには、次のコマンドを使用します。

```
OS10(config)# do show running-configuration | grep simple
service simple-password
```

[強力なパスワードの強制]

[論拠]: デフォルトでは、構成するパスワードは 9 文字以上の英数字と特殊文字を含んでいる必要があります。さらにパスワードの強度を上げるには、異なる文字の組み合わせを使用し、パスワードを長くするようユーザーに強制します。

[構成]:

```
OS10(config)# password-attributes {[min-length number] [character-restriction {[upper number]
[lower number][numeric number] [special-char number]}}
OS10(config)# exit
OS10# write memory
```

- `min-length` *number* :(オプション) 必要な英数字の最小文字数を、6 ~ 32 文字の間で設定します。デフォルトは 9 文字です。
- `character-restriction`:
  - `upper` *number* :(オプション) 必要な大文字の最小文字数を、0 ~ 31 文字の間で設定します。デフォルトは 0 です。
  - `lower` *number* :(オプション) 必要な小文字の最小数を、0 ~ 31 文字の間で設定します。デフォルトは 0 です。
  - `numeric` *number* :(オプション) 必要な数字の最小文字数を、0 ~ 31 文字の間で設定します。デフォルトは 0 です。
  - `special-char` *number* :(オプション) 必要な特殊文字の最小数を、0 ~ 31 文字の間で設定します。デフォルトは 0 です。

パスワードを選択する場合、Dell EMC ネットワーキングは、覚えるのが難しい複雑なパスワードを使用するのではなく、複数の、覚えやすい一般的な言葉をパスワードに使用することを推奨します。覚えやすい複数の単語を合わせて、特殊文字と数字を使用してパスフレーズを変更することで、パスワードを完成させることができます。例えば、`correcthorsebatterystaple` の代わりに `C0rr3c+h0r5e8atTerystapl3` を使用できます。

メモ: 管理者パスワードを含む、OS10 ユーザー名のパスワードを紛失または忘れた場合の復旧方法については、「OS10 ユーザー名のパスワードの復旧」を参照してください。

[パスワードの不明瞭化]

[論拠]: ユーザーが実行中の構成を表示すると、暗号化された形式でパスワードが表示されます。テキスト文字が表示されないように、`show` コマンドの出力でパスワードを不明瞭にします。

[構成]:

```
OS10(config)# service obscure-password
OS10(config)# exit
OS10# write memory
OS10# show running-configuration users
username admin password **** role sysadmin priv-lvl 15
username desk1 password **** role sysadmin priv-lvl 15
```

Federal Information Processing Standards (FIPS)

FIPS は、連邦政府暗号化アルゴリズムで特定の機能を使用する方法を定義する、連邦標準のセットです。

[ご使用の環境で FIPS が必要な場合に有効化する]

[論拠]: FIPS を有効にすると、FIPS 対応アプリケーション (TLS 経由の RADIUS など) によって使用される証明書キー ペアが FIPS 準拠としてインストールされます。

[構成]:

```
OS10# crypto fips enable
OS10# write memory
```

[FIPS が有効になっているかどうかのチェック]

システムで FIPS が有効になっているかどうかを確認するには、次のコマンドを使用します。

```
OS10# show fips status

FIPS mode:                    Disabled
```

セキュア ブートの有効化と構成

OS10 セキュア ブートにより、OS10 イメージの信頼性と整合性を検証するためのメカニズムが提供されます。セキュア ブートでは、起動プロセス中に悪意のあるコードが読み込まれて実行されないようにシステムを保護します。セキュア ブート機能を使用して、インストール中およびいつでもオン デマンドで OS10 イメージを検証します。

[セキュア ブートの有効化]

[論拠]: セキュア ブート機能を有効にすると、侵害されたカーネルとシステム バイナリーが起動操作中にロードされるのを防ぐことができます。

[構成]:

```
OS10(config)# secure-boot enable
OS10(config)# exit
OS10# write memory
```

[スタートアップ構成ファイルの保護]

[論拠]: スタートアップ構成ファイルを保護することで、現在のスタートアップ設定ファイルの保護されたコピーを内部で保存できます。スイッチの起動中に、保護されているバージョンの起動構成がロードされます。スタートアップ構成ファイルを保護することにより、システムの起動時に、侵害された構成ファイルがロードされないようにすることができます。

[構成]:

```
OS10(config)# secure-boot protect startup-config
OS10(config)# exit
OS10# write memory
```

[オン デマンドでの OS10 イメージ ファイルの検証]

[論拠]: OS10 イメージ ファイルの署名を検証して、OS10 イメージが侵害されていないことを確認します。

[構成]:

```
OS10# image verify image-filepath {sha256 signature signature-filepath | gpg signature
signature-filepath | pki signature signature-filepath public-key key-file}
```

[OS10 カーネル、システム バイナリー、およびスタートアップ構成ファイルの検証]

[論拠]: システム起動時に、OS10 カーネル バイナリー イメージ、システム バイナリー ファイル、およびスタートアップ構成ファイルを検証します。スタートアップ時にこれらのファイルを検証することにより、システムが侵害されたファイルをロードしないようにします。

[構成]:

```
OS10# secure-boot verify {kernel | file-system-integrity | startup-config}
```

[OS10 アップグレード イメージ ファイルの検証]

[論拠]: OS10 アップグレードをインストールする前に、イメージ ファイルのデジタル署名を検証します。インストールする前に、次のコマンドを使用して OS10 イメージを検証できます。

[構成]:

```
OS10# image secure-install image-filepath {sha256 signature signature-filepath | gpg
signature signature-filepath | pki signature signature-filepath public-key key-file}
```

メモ: セキュア ブートが有効になっている場合は、`image secure-install` コマンドを使用した場合にのみ、OS10 のアップグレードを行うことができます。

[ONIE OS 手動インストール前の OS10 イメージの検証]

[論拠]: セキュア ブートが有効になっていて、ONIE を使用して OS10 イメージを手動でインストールする場合は、PKI または SHA256 を使用してイメージを検証できます。

[構成]:

```
OS10# onie-nos-install image_url pki signature_filepath certificate_filepath
```

または

```
OS10# onie-nos-install image_url sha256 signature_filepath
```

[セキュア ブートの有効化とファイルの整合性ステータスのチェック]

次のコマンドを使用して、セキュア ブート操作のステータスとファイルの整合性ステータスをチェックします。

```
OS10# show secure-boot status
Last boot was via secure boot     : yes
Secure boot configured          : yes
Latest startup config protected     : yes
OS10# show secure-boot file-integrity-status
File Integrity Status: OK
```

ユーザー、役割、権限レベル

パスワードを使用して、スイッチへのターミナル アクセスを制御します。ただし、権限レベルを使用してコマンドのサブセットへのユーザー アクセスを制限することで、セキュリティを強化できます。

[ユーザーの作成、役割の割り当て、権限レベルの作成]

[論拠]: スイッチへのターミナル アクセスの制御は、デバイスとネットワークを保護する方法の 1 つです。セキュリティを強化するために、権限レベルを使用してコマンドのサブセットへのユーザー アクセスを制限できます。

[構成]:

- CONFIGURATION モードで権限レベルを作成します。

  ```
  OS10(config)# privilege mode priv-lvl privilege-level command-string
  ```

  - *mode* : CLI モードへのアクセスに使用する権限モードを入力します。
    - `exec` : EXEC モードにアクセスします。
    - `configure` : クラスマップ、DHCP、ログ、監視、openFlow、ポリシーマップ、QOS、support-assist、テレメトリー、CoS、Tmap、UFD、VLT、VN、VRF、WRED、エイリアス モードにアクセスします。
    - `interface` : Ethernet、FibreChannel、ループバック、管理、null、ポートグループ、lag、ブレークアウト、範囲、ポート チャネル、VLAN モードにアクセスします。
    - `route-map` : ルートマップ モードにアクセスします。
    - `router` : `router-bgp` モードおよび `router-ospf` モードにアクセスします。
    - `line` : line-vty モードにアクセスします。
  - `priv-lvl` *privilege-level* : 権限レベルの数を 2 ~ 14 の範囲で入力します。
  - *command-string* : 権限レベルでサポートされているコマンドを入力します。
- ユーザー名、パスワードを作成して役割を割り当て、CONFIGURATION モードで権限レベルを割り当てます。

  ```
  OS10(config)# username username password password role role priv-lvl privilege-level
  ```

  - `username` *username* : 最大 32 文字の英数字、最低 1 文字以上のテキスト文字列を入力します。
  - `password` *password* : 最大 32 文字の英数字、最低 9 文字以上のテキスト文字列を入力します。
  - `role` *role* : ユーザーの役割を入力します。
    - `sysadmin` : システム内のすべてのコマンドへのフル アクセス、ファイル システムを操作するコマンドへの排他的アクセス、システム シェルへのアクセスが可能です。システム管理者は、ユーザー ID とユーザーの役割を作成できます。

- secadmin：パスワードの強度、AAA 認証、暗号形式キーなどのセキュリティ ポリシーとシステム アクセスを設定する、構成コマンドへのフル アクセスが可能です。セキュリティ管理者は、暗号形式キー、ログイン統計情報、ログ情報などのセキュリティ情報を表示できます。
- netadmin：ルート、インターフェイス、ACL など、スイッチ経由のトラフィックの流れを管理する構成コマンドへのフル アクセスが可能です。ネットワーク管理者は、セキュリティ機能の構成コマンドにアクセスすることも、セキュリティ情報を表示することもできません。
- netoperator：現在の構成を表示するために EXEC モードにアクセスします。ネットワーク オペレーターは、スイッチの構成設定を変更することはできません。

○ priv-lvl *privilege-level*：権限レベルを 0 ~ 15 の範囲で入力します。
- レベル 0：ユーザーに最低限の権限を与え、基本的なコマンドへのアクセスを制限します。
- レベル 1：一連の show コマンドや、ping、traceroute などの特定の操作へのアクセスを提供します。
- レベル 15：使用可能なすべてのコマンドへのアクセスを提供します。これは、sysadmin の役割で許可されているコマンドと同等です。
- レベル 0、1、15：事前に定義されたコマンド セットが適用される、システムにより構成された権限レベルです。
- レベル 2 ~ 14：構成されていません。これらのレベルは、さまざまなユーザーやアクセス権に合わせてカスタマイズすることができます。

- CONFIGURATION モードで各権限レベルの有効パスワードを構成します。権限レベルを切り替えて、各レベルでサポートされているコマンドにアクセスするには、enable password コマンドを使用します。

```
OS10(config)# enable password encryption-type password-string priv-lvl privilege-level
OS10(config)# exit
OS10# write memory
```

○ *encryption-type*：パスワード入力の暗号化タイプを入力します。
- 0：パスワード暗号化なしのプレーン テキストを使用します。
- sha-256：SHA-256 アルゴリズムを使用してパスワードを暗号化します。
- sha-512：SHA-512 アルゴリズムを使用してパスワードを暗号化します。

メモ: パスワードに sha-256 または sha512 の暗号化を使用していることを確認します。

○ priv-lvl *privilege-level*：権限レベルを 1 ~ 15 の範囲で入力します。

メモ: パスワードの暗号化には、SHA-256 または SHA-512 を使用します。

```
OS10(config)# privilege exec priv-lvl 12 "show version"
OS10(config)# privilege exec priv-lvl 12 "configure terminal"
OS10(config)# privilege configure priv-lvl 12 "interface ethernet"
OS10(config)# privilege interface priv-lvl 12 "ip address"
OS10(config)# username delluser password $6$Yij02Phe2n6whp7b$ladskj0HowijIlkajg981 role
secadmin priv-lvl 12
OS10(config)# enable password sha-256 $5$2uThib1o$84p.tykjmz/w7j26ymoKBjrb7uepkUB priv-lvl 12
OS10(config)# exit
OS10# write memory
```

[ユーザーとその役割の表示]

次に、ローカル システム上で構成されているユーザー、その役割、割り当てられた権限レベルを示します。

```
OS10# show running-configuration users
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/3OJc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH. role sysadmin priv-lvl 15
OS10# show running-configuration userrole
```

ポート セキュリティ

ポート セキュリティ機能を使用して、インターフェイスを介してトラフィックを送信できるワークステーションの数を制限したり、MAC アドレスの移動を制御したりすることができます。ポート セキュリティは、システムのセキュリティを強化する次のサブ機能を含むパッケージです。

1. MAC アドレス学習制限（MLL）
2. スティッキー MAC
3. MAC アドレス移動制御

[MAC アドレス学習制限の構成]

[論拠]: MAC アドレス学習制限の方式を使用すると、インターフェイス上で許可される MAC アドレスの上限値を設定できます。MAC アドレスを制限することで、スイッチを MAC アドレス フラッディング攻撃から保護します。インターフェイス上で構成された制限に達すると、デフォルトでは、システムは不明なデバイスからのすべてのトラフィックをドロップします。インターフェイスでポート セキュリティを有効にした後、インターフェイスは、デフォルトで 1 個のセキュア MAC アドレスを学習できます。この制限は、セキュア ダイナミック MAC アドレスとセキュア スタティック MAC アドレスの両方に適用されます。

[構成]:

1. CONFIGURATION モードでシステムのポート セキュリティを有効にします。

```
OS10(config)# switchport port-security
```

2. CONFIGURATION モードでインターフェイスのポート セキュリティを有効にします。

```
OS10(config)# switchport port-security
OS10(config)# no disable
```

3. インターフェイスが INTERFACE PORT SECURITY モードで学習できるセキュア MAC アドレスの数を構成します。

```
mac-learn {limit | no-limit}
```

`limit` キーワードでの範囲は 0 ~ 3072 です。ハードウェアでサポートされている MAC アドレスの最大数をインターフェイスが学習できるようにするには、`no-limit` キーワードを使用します。

[MAC アドレス学習制限の例]

```
OS10# configure terminal
OS10(config)#interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport port-security
OS10(config-if-port-sec)# no disable
OS10(config-if-port-sec)# mac-learn limit 100
OS10(config-if-port-sec)# end
OS10# write memory
```

[MAC アドレス学習制限違反のアクションの構成]

[論拠]: セキュア MAC アドレスの数が構成された最大値に達すると、学習した MAC アドレスとは異なる送信元 MAC アドレスのフレームをインターフェイスが受信した場合、システムは MAC アドレス学習制限の違反とみなします。

[構成]:

INTERFACE PORT SECURITY モードでは、次のコマンドを使用します。

- 違反の原因となった MAC アドレスを表示するには、`log` オプションを使用します。また、システムはパケットをドロップします。

```
OS10(config-if-port-sec)#mac-learn limit violation log
```

- MAC アドレス学習制限の違反が発生したときにパケットをドロップするには、`drop` オプションを使用します。

```
OS10(config-if-port-sec)#mac-learn limit violation drop
```

- MAC アドレス学習制限の違反が発生したときにパケットを転送するには、`flood` オプションを使用します。システムは MAC アドレスを学習しません。

```
OS10(config-if-port-sec)#mac-learn limit violation forward
```

- MAC アドレス学習制限違反のインターフェイスをシャット ダウンするには、`shutdown` オプションを使用します。

```
OS10(config-if-port-sec)#mac-learn limit violation shutdown
```

[MAC アドレス学習制限違反のアクションの構成例]

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport port-security
OS10(config-if-port-sec)# no disable
OS10(config-if-port-sec)# mac-learn limit 100
OS10(config-if-port-sec)# mac-learn limit violation shutdown
OS10(config-if-port-sec)# end
OS10# write memory
```

[スティッキー MAC アドレスの構成]

[論拠]: システムを再ロードすると、ポート セキュリティは動的に学習したセキュア MAC アドレスを削除します。スティッキー機能を使用して、動的に学習したセキュア MAC アドレスをシステムの再起動後も保持できます。これにより、インターフェイスがこれらの MAC アドレスを再び学習する必要がなくなります。

[構成]:

INTERFACE PORT SECURITY モードで、次のコマンドを入力します。

```
sticky
```

メモ: スティッキー MAC アドレスの学習を有効にする前に、インターフェイスが `mac-learn limit` コマンドを使用して学習できる MAC アドレスの数を制限するようにしてください。

[スティッキー MAC アドレスの構成例]

```
OS10# configure terminal
OS10(config)#interface ethernet 1/1/1
OS10(config-if-eth1/1/1)#switchport port-security
OS10(config-if-port-sec)#no disable
OS10(config-if-port-sec)#mac-learn limit 100
OS10(config-if-port-sec)#sticky
OS10(config-if-port-sec)# end
OS10# write memory
```

[MAC アドレスの移動]

[論拠]: MAC アドレスの移動は、システムが同じブロードキャスト ドメイン上の別のポート セキュリティ有効インターフェイスを通じてすでに学習したインターフェイス上で、同じ MAC アドレスを検出した場合に発生します。MAC アドレスの移動は、セキュア スタティック MAC アドレスおよびスティッキー MAC アドレスに対しては許可されません。デフォルトでは、動的に学習した MAC アドレスの MAC アドレス移動は、システムで無効になっています。セキュア ダイナミック MAC アドレスの移動は、ポートセキュリティ有効インターフェイスとポートセキュリティ無効インターフェイス間で許可されています。

[構成]:

INTERFACE PORT SECURITY モードでは、次のコマンドを使用します。

```
OS10(config-if-port-sec)#mac-move allow
OS10(config-if-port-sec)# end
OS10# write memory
```

[MAC アドレス移動の構成例]

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport port-security
OS10(config-if-port-sec)# no disable
OS10(config-if-port-sec)# mac-learn limit 100
OS10(config-if-port-sec)# mac-move allow
OS10(config-if-port-sec)# end
OS10# write memory
```

[MAC アドレス移動違反アクションの構成]

[論拠]: システムが、別のポートセキュリティ有効インターフェイスを通じてすでに学習した MAC アドレスと同じ MAC アドレスをポートセキュリティ有効インターフェイスで検出した場合、デフォルトでは、MAC アドレス移動違反とみなされます。MAC アドレス移動違反アクションを構成できます。また、ポート セキュリティ有効インターフェイス間で MAC アドレスを移動できるようにシステムを構成することもできます。

[構成]:

- 違反の原因となった MAC アドレスを表示するには、`log` オプションを使用します。また、システムはパケットをドロップします。

  ```
  OS10(config-if-port-sec)#mac-move violation log
  ```

- MAC アドレス移動違反が発生したときにパケットをドロップするには、`drop` オプションを使用します。

  ```
  OS10(config-if-port-sec)#mac-move violation drop
  ```

- MAC 移動違反時に、MAC アドレスを学習した元のインターフェイスをシャット ダウンするには、`shutdown-original` オプションを使用します。

```
OS10(config-if-port-sec)#mac-move violation shutdown-original
```

- 別のインターフェイスによってすでに学習されている MAC アドレスを検出したインターフェイスをシャット ダウンするには、`shutdown-offending` オプションを使用します。

```
OS10(config-if-port-sec)#mac-move violation shutdown-offending
```

- 元のインターフェイスと、問題のあるインターフェイスの両方をシャット ダウンするには、 `shutdown-both` オプションを使用します。

```
OS10(config-if-port-sec)#mac-move violation shutdown-both
```

[有効かつ実行中のポート セキュリティ機能の確認]

すべてのインターフェイスでポート セキュリティが有効になっているかどうかを確認するには、次のコマンドを使用します。このコマンドにより、ポート セキュリティ機能のステータスに関する情報も表示されます。個別のインターフェイスに関する詳細を表示するには、特定のインターフェイスを指定します。

```
OS10# show switchport port-security interface erthernet 1/1/1
Global Port-security status       : Enabled

Interface name                    : ethernet1/1/1

Port Security                     : Enabled
Port Status                       : Up
Mac learn limit                   : 100
MAC-learn-limit-Violation action  : Log
Sticky                            : Disabled
Mac-move-allow                    : Not Allowed
Mac-move-violation action         : shutdown-both
Aging                             : Enabled
Total MAC Addresses               : 10
Secure static MAC Addresses       : 0
Sticky MAC Addresses              : 10
Secure Dynamic MAC addresses      : 0
```

管理プレーン

これらの設定は、OS10 のサービス、設定、構成サービスに適用されます。

役割ベースのアクセス制御

役割ベースのアクセス制御（RBAC）により、アクセスと認可を制御できます。定義された役割に基づいて、ユーザーに権限が与えられます。ユーザーによるシステムへの適切なアクセスを許可するために、ジョブ機能に基づいてユーザーの役割を作成します。ユーザーに割り当てることができる役割は 1 個だけで、多くのユーザーに同じ役割を割り当てることができます。ユーザーの役割により、ログイン時にユーザーが認証および承認されます。

[AAA ログイン認証の有効化]

[論拠]: 認証、承認、アカウンティング（AAA）サービスにより、不正アクセスからネットワークが保護されます。AAA は、システムにアクセスするユーザーに対するアクセス制御の一元化された手段です。

[構成]:

```
OS10(config)# aaa authentication login {console | default} local
OS10(config)# exit
OS10# write memory
```

- `console`：コンソール ログインの認証方法を構成します。
- `default`：SSH および Telnet ログインの認証方法を構成します。
- `local`：`username password role` コマンドで構成されたローカル ユーザー名、パスワード、役割エントリーを使用します。

[フォールバック オプションを使用した AAA ログイン認証の有効化]

[論拠]: フォールバック オプションを使用した AAA 認証の構成により、認証時に耐久性が提供されます。1 つの方法で障害が発生した場合、システムは他の認証方法を使用します。

[構成]:

```
OS10(config)# aaa authentication login {console | default} {local | group radius | group
tacacs+}
OS10(config)# exit
OS10# write memory
```

- `console` : コンソール ログインの認証方法を構成します。
- `default` : SSH および Telnet ログインの認証方法を構成します。
- `local` : `username password role` コマンドで構成されたローカル ユーザー名、パスワード、役割エントリーを使用します。
- `group radius` : `radius-server host` コマンドで構成された RADIUS サーバーを使用します。
- `group tacacs+` : `tacacs-server host` コマンドで構成された TACACS+サーバーを使用します。

メソッド リストにある認証方法は、構成された順序で作動します。

[コマンドへの AAA アカウンティングの有効化]

[論拠]: コマンドへの AAA アカウンティングにより、Telnet や SSH などのコンソール接続とリモート接続に関するログインおよびコマンド情報が記録されます。

[構成]:

```
OS10(config)# aaa accounting commands all {console | default} {start-stop | stop-only | none}
[logging] [group tacacs+]
OS10(config)# exit
OS10# write memory
```

- `commands all` : ユーザーによって入力されたすべてのコマンドを記録します。RADIUS アカウンティングでは、このオプションはサポートされません。
- `console` : コンソール接続の OS10 セッションで、すべてのユーザー認証とログイン、またはすべてのユーザー入力コマンドを記録します。
- `default` : Telnet や SSH などによるリモート接続の OS10 セッションで、すべてのユーザーの認証とログイン、またはすべてのユーザー入力コマンドを記録します。
- `start-stop` : プロセスの開始時に開始通知を送信し、プロセスの終了時に停止通知を送信します。
- `stop-only` : プロセスが終了したときに、停止通知のみを送信します。
- `none` : アカウンティング通知は送信されません。
- `logging` : Syslog のすべてのアカウンティング通知をログに記録します。
- `group tacacs+` : 最初に到達可能な TACACS+サーバーのすべてのアカウンティング通知をログに記録します。

[認証イベントに対する AAA アカウンティングの有効化]

[論拠]: 認証イベントに対する AAA アカウンティングにより、Telnet や SSH などのコンソール接続とリモート接続に関するログインおよびコマンド情報が記録されます。

[構成]:

```
OS10(config)# aaa accounting exec {console | default} {start-stop | stop-only | none}
[logging] [group tacacs+]
OS10(config)# exit
OS10# write memory
```

- `console` : コンソール接続の OS10 セッションで、すべてのユーザー認証とログイン、またはすべてのユーザー入力コマンドを記録します。
- `default` : Telnet や SSH などによるリモート接続の OS10 セッションで、すべてのユーザーの認証とログイン、またはすべてのユーザー入力コマンドを記録します。
- `start-stop` : プロセスの開始時に開始通知を送信し、プロセスの終了時に停止通知を送信します。
- `stop-only` : プロセスが終了したときに、停止通知のみを送信します。
- `none` : アカウンティング通知は送信されません。
- `logging` : Syslog のすべてのアカウンティング通知をログに記録します。
- `group tacacs+` : 最初に到達可能な TACACS+サーバーのすべてのアカウンティング通知をログに記録します。

メソッド リストにある認証方法は、構成された順序で作動します。

[AAA 再認証または有効モードの有効化]

[論拠]: ユーザーがリソースにアクセスできないようにしたり、ユーザーが実行できないタスクを実行したり、認証方法またはサーバーの変更時にログによるユーザーの再認証を要求したりすることができます。

[構成]:

```
OS10(config)# aaa re-authenticate enable
```

[RADIUS 認証の構成]

[論拠]: 従来の RADIUS ベースのユーザー認証は UDP を介して実行され、安全な通信のために MD5 メッセージダイジェスト アルゴリズムが使用されます。RADIUS ユーザー認証交換のセキュリティを強化するため、RFC 6614 では、トランスポート レイヤー セキュリティ (TLS) プロトコルを使用して RADIUS を定義します。RADIUS over TLS は、認証交換全体を TLS 接続で保護し、セキュリティを強化します。

[構成]:

```
OS10(config)# radius-server host {hostname | ip-address} tls security-profile profile-name
[auth-port port-number] key {0 authentication-key | 9 authentication-key | authentication-key}
OS10(config)# exit
OS10# write memory
```

- *hostname* : RADIUS サーバーのホスト名を入力します。
- *ip-address* : RADIUS サーバーの IPv4 (A.B.C.D) または IPv6 (x:x:x:x::x) アドレスを入力します。
- tls security-profile *profile-name* : RADIUS サーバーでの TLS 認証に使用するために、スイッチ上で X.509v3 証明書を使用するためのセキュリティ プロファイルを入力します。
- key 0 *authentication-key* : プレーン テキストで認証キーを入力します。最大 42 文字です。
- key 9 *authentication-key* : 暗号化形式で認証キーを入力します。最大 128 文字です。
- *authentication-key*: プレーン テキストで認証を入力します。最大 42 文字です。キーの前に 0 を入力する必要はありません。
- auth-port *port-number* :(オプション)サーバーで認証用に使用される UDP ポート番号を 0 ~ 65535 の範囲で入力します。デフォルトは 1812 です。
- key *authentication-key* :(オプション) サーバー上のデバイスを認証するための認証キーを入力します。最大 42 文字です。デフォルトは radius_secure です。

[RADIUS 認証再試行の構成]

[論拠]: OS10 が RADIUS 認証要求を再送する回数を構成します。不要な再試行を回避するには、小さい値を構成します。

[構成]:

```
OS10(config)# radius-server retransmit retries
OS10(config)# exit
OS10# write memory
```

retries : 再試行回数を 0 ~ 100 の範囲で入力します。

[TACACS+認証の構成]

[論拠]: TACACS+サーバーからの認証応答を待機するために使用するグローバル タイムアウトを構成します。待機時間が長くなるのを防ぐため、小さい値を構成します。

[構成]:

```
OS10(config)# tacacs-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
OS10(config)# exit
OS10# write memory
```

- *hostname* : RADIUS サーバーのホスト名を入力します。
- *ip-address* : RADIUS サーバーの IPv4 (A.B.C.D) または IPv6 (x:x:x:x::x) アドレスを入力します。
- 0 *authentication-key* : プレーン テキストで認証キーを入力します。最大 42 文字です。
- 9 *authentication-key* : 暗号化形式で認証キーを入力します。最大 128 文字です。
- *authentication-key*: プレーン テキストで認証を入力します。最大 42 文字です。キーの前に 0 を入力する必要はありません。
- auth-port *port-number* :(オプション)サーバーで認証用に使用される UDP ポート番号を 0 ~ 65535 の範囲で入力します。デフォルトは 1812 です。

- *authentication-key*:(オプション)サーバー上のスイッチを認証するために使用する認証キーを入力します。最大 42 文字です。デフォルトは radius_secure です。

[TACACS+認証応答タイマーの構成]

[論拠]: TACACS+サーバーからの認証応答を待機するために使用するグローバル タイムアウトを構成します。待機時間が長くなるのを防ぐため、小さい値を構成します。

[構成]:

```
OS10(config)# tacacs-server timeout seconds
OS10(config)# exit
OS10# write memory
```

seconds : TACACS+サーバーからの認証応答を待機するために使用されるタイムアウト時間を、1 ~ 1000 秒の範囲で入力します。

[RBAC 構成の表示]

システムで構成された RBAC を表示するには、次のコマンドを使用します。

```
OS10# show running-configuration aaa
aaa authentication login default group radius local
aaa authentication login console local
```

アクセス ルール

安全なアクセス ルールを構成します。

[リモート システム アクセスに対して SSH のみを有効にする]

[論拠]: OS10 のデフォルトでは、SSH のみがリモート システム アクセス用に有効になっています。Telnet プロトコルは安全ではないため、Dell EMC は、Telnet サーバーを有効にしないことを推奨します。

メモ: SSH サーバーを無効にしていた場合は、再度有効にし、Telnet サーバーを無効にします。リモート システム アクセスには、常に SSH を使用します。

[構成]:

```
OS10(config)# ip ssh server enable
OS10(config)# ip ssh server max-auth-tries 4
OS10(config)# no ip telnet server enable
OS10(config)# exit
OS10# write memory
```

[SSH アクセス制御の有効化]

[論拠]: アクセス リストを使用してスイッチへの SSH 接続をフィルタリングします。

[構成]:

```
OS10(config)# ip access-list permit10
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
OS10(config-ipv4-acl)# exit
OS10(config)# line vty
OS10(config-line-vty)# ip access-class permit10
OS10(config-line-vty)# exit
OS10(config)# exit
OS10# write memory
```

[EXEC セッション タイムアウトの構成]

[論拠]: デフォルトでは、EXEC タイムアウトは構成されていません。EXEC モードへの不正アクセスを防止するには、タイムアウト インターバルを構成します。

[構成]:

```
OS10(config)# exec-timeout timeout-value
OS10(config)# exit
OS10# write memory
```

timeout-value : 現在のセッションを切断するまでの、システム上の非アクティブな秒数を指定します (0 ~ 3600)。

[コンカレント ログイン セッションの制限]

[論拠]: 同じユーザー ID で 1 台のスイッチ上のアクティブ セッション数が無制限にならないようにするため、コンソールとリモート接続の数を制限します。

[構成]:

```
OS10(config)# login concurrent-session limit-number
OS10(config)# exit
OS10# write memory
```

limit-number: 任意のユーザーがコンソールまたは仮想端末の回線で使用できるコンカレント セッションの数を指定します (1 ~ 12)。

[ユーザーのロックアウトの確認]

[論拠]: 指定された回数のログイン試行が失敗した後に、ユーザーが特定の時間にわたってシステムにログ インできないようにシステムを構成します。

[構成]:

```
OS10(config)# password-attributes max-retry number lockout-period minutes
OS10(config)# exit
OS10# write memory
```

- `max-retry` *number*:(オプション) ユーザーがロック アウトされるまでの、連続したログイン試行失敗の最大回数を、0 ~ 16 の範囲で構成します。
- `lockout-period` *minutes*:(オプション) ログイン試行失敗の最大回数を超過した場合に、そのユーザー ID がシステムにアクセスすることを禁止する時間を 0 ~ 43,200 の範囲で設定します。

[ログイン統計の有効化]

[論拠]: ログインに成功した回数や失敗した回数、役割の変更、ユーザーが最後にログ インした時間などのユーザー ログイン情報を表示するには、ログインが成功した後にログイン統計を有効にします。ログイン統計を有効にした後、`show login statistics {all | user}`コマンドを使用してユーザーのログイン情報を表示できます。

[構成]:

```
OS10(config)# login-statistics enable
OS10(config)# exit
OS10# write memory
```

バナー ルール

ユーザーがシステムにログ インする前後に、メッセージを表示します。これらのメッセージにより、法律上の権限をユーザーに伝えたり、ユーザーが使用ポリシーに同意したものとみなしたりすることができます。

[ログイン バナーの有効化]

[論拠]: ログイン バナーは、ユーザーがシステムへのログ インを試行したときにユーザーに表示されます。

[構成]:

```
OS10(config)# banner login %
DellEMC S4148U-ON login
Enter your username and password
%
OS10(config)# exit
OS10# write memory
```

[ログイン バナーの有効化]

[論拠]: ログイン バナーは、ユーザーがシステムにログ インした後に表示されます。

[構成]:

```
OS10(config)# banner motd %
DellEMC S4148U-ON login
Enter your username and password
%
```

```
OS10(config)# exit
OS10# write memory
```

SNMP ルール

Simple Network Management Protocol (SNMP) へのアクセス制限により、SNMP を使用する際のデバイスのセキュリティが向上します。

[特定の SNMP コミュニティーへの読み取り/書き込みアクセスの禁止]

[論拠]: 単一または複数の SNMP コミュニティーへの読み取り/書き込みアクセスを禁止して、不正なエンティティーがデバイスをリモートで操作できないようにします。

[構成]:

```
OS10(config)# no snmp-server community community_string {ro | rw}
OS10(config)# exit
OS10# write memory
```

[ACL なしの SNMP へのアクセスを禁止]

[論拠]: ACL が構成されていない場合、有効な SNMP コミュニティー文字列を持つユーザーは誰でもシステムにアクセスでき、不要な変更を加える可能性があります。信頼できるステーションの許可されたグループのみがシステムへの SNMP アクセスを行えるように、ACL を定義して適用します。

[構成]:

```
OS10(config)# snmp-server community name {ro | rw} acl acl-name
OS10(config)# exit
OS10# write memory
```

```
OS10(config)# ip access-list snmp-read-only-acl
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
OS10(config-ipv4-acl)# exit
OS10(config)# snmp-server community public ro acl snmp-read-only-acl
OS10(config)# exit
OS10# write memory
```

[SNMP v3 の構成]

[論拠]: SNMP v2 は暗号化または認証をサポートしていません。Dell EMC Networking は、SNMP リソースへの安全なアクセスをサポートする SNMP v3 を使用することを強く推奨します。

[構成]:

- SNMP エンジン ID を構成します。`snmp-server engineID [local engineID] [remote ip-address {[udp-port port-number] remote-engineID}]`
  - `local engineID`: スイッチのローカル SNMP エージェントを識別するエンジン ID を、オクテットのコロン区切りの数字で入力します。最大 27 文字です。
  - `remote ip-address`: ローカル SNMP エージェントにアクセスするリモート SNMP デバイスの IPv4 または IPv6 アドレスを入力します。
  - `udp-port port-number`: リモート デバイスの UDP ポート番号を 0 ~ 65535 の範囲で入力します。
  - `remote-engineID`: リモート デバイス上の SNMP エージェントを識別するエンジン ID を、`0x` および 16 進数の文字列で入力します。
- SNMP の表示を構成します。

  ```
  OS10(config)# snmp-server view view-name oid-tree [included | excluded]
  ```

  - `view-name`: 読み取り専用、読み取り/書き込み、または通知ビューの名前を入力します。最大 32 文字です。
  - `oid-tree`: ビューが 12 オクテットのドット区切り形式で始まる SNMP オブジェクト ID を入力します。
  - `included`:(オプション) ビューに MIB ファミリーを含めます。
  - `excluded`:(オプション) MIB ファミリーをビューから除外します。
- SNMP グループを構成します。

  ```
  OS10(config)# snmp-server group group-name v3 security-level [read view-name] [write view-name] [notify view-name]
  ```

- *group-name*：グループの名前を入力します。最大 32 文字の英数字です。
- v3 *security-level*：SNMPv3 では、オプションで SNMP メッセージのユーザー認証と暗号化を行うことができます。snmp-server user コマンドで構成します。
- security-level：(SNMPv3 のみ) SNMPv3 ユーザーのセキュリティ レベルを構成します。
  - auth：SNMP メッセージでユーザーを認証します。
  - noauth：ユーザーの認証や SNMP メッセージの暗号化を行いません。メッセージをプレーン テキストで送信します。
  - priv：ユーザーの認証、SNMP メッセージの暗号化または復号化を行います。
- access *acl-name* (オプション) IPv4 または IPv6 アクセス リストの名前を入力して、スイッチで受信した SNMP リクエストをフィルタリングします。最大 16 文字です。
- read *view-name*：(オプション) 読み取り専用ビューの名前を入力します。最大 32 文字です。
- write *view-name*：(オプション) 読み取り/書き込みビューの名前を入力します。最大 32 文字です。
- notify *view-name*：(オプション) 通知ビューの名前を入力します。最大 32 文字です。

- SNMP ユーザーを構成します。

```
OS10(config)# snmp-server user user-name group-name security-model localized auth sha auth-
password priv aes priv-password
OS10(config)# exit
OS10# write memory
```

- *user-name*：ユーザーの名前を入力します。最大 32 文字の英数字です。
- *group-name*：ユーザーが属しているグループの名前を入力します。最大 32 文字の英数字です。
- *security-model*：SNMP メッセージのセキュリティ レベルを設定する SNMP バージョンを入力します。
  - 3：SNMPv3 は、SNMP メッセージのユーザー認証と暗号化を行います。
- auth：(SNMPv3 のみ) ユーザーに送信される SNMPv3 メッセージにユーザー認証キーを含めます。
  - sha：SHA アルゴリズムを使用して認証キーを生成します。
  - *auth-password*：暗号化された文字列を入力します。
- priv：ユーザーに送信される SNMPv3 メッセージの暗号化を構成します。
  - aes：AES 128 ビット アルゴリズムを使用してメッセージを暗号化します。
  - *priv-password*：暗号化された文字列を入力します。
- localized：ローカライズされたキーの形式で SNMPv3 認証キーおよび/またはプライバシー キーを生成します。

[実行されている SNMP ルールのチェック]

```
OS10# show running-configuration snmp
!
snmp-server community public ro acl snmp-read-only-acl
```

コントロール プレーン

コントロール プレーンには、モニタリング、ルート テーブルのアップデート、システムの動的な操作が含まれます。

システム クロック ルール

これらのシステム クロック ルールにより、デバイスの時刻とタイムスタンプの設定が強制されます。

[タイムゾーンを協定世界時 (UTC) に設定]

[論拠]: デフォルトでは、システムのタイム ゾーンは UTC に設定されています。デフォルトのタイム ゾーンが変更された場合は、UTC に設定します。システム タイム ゾーンを UTC に設定すると、異なるタイム ゾーン間で起きる問題のトラブルシューティングが容易になります。

[構成]:

```
OS10(config)# clock timezone standard-timezone UTC
OS10(config)# exit
OS10# write memory
```

ログ ルール

ログを使用して、エラーや情報の通知、セキュリティ監査、ネットワーク フォレンジックを行うことができます。

[コンソールでのログの有効化]

[論拠]: コンソールへのログ記録を有効にし、ログ メッセージがシステム パフォーマンスに影響しないように、重大度を「重要」に制限します。

[構成]:

```
OS10(config)# logging console enable
OS10(config)# logging console severity log-crit
OS10(config)# exit
OS10# write memory
```

[TLS 経由での Syslog サーバーへのログの有効化]

[論拠]: Syslog サーバーへのログを有効にし、TLS で接続を保護します。

[構成]:

```
OS10(config)# logging server {hostname | ipv4-address | ipv6-address} tls [port-number]
[severity severity-level] [vrf {management | vrf-name]
OS10(config)# exit
OS10# write memory
```

- *ipv4-address | ipv6-address* :(オプション) ログ サーバーの IPv4 または IPv6 アドレスを入力します。
- tls *port-number* :(オプション) リモート ログ サーバーの指定したポート (1 ~ 65535) に、TCP、UDP、TLS 転送を使用して Syslog メッセージを送信します。
- *severity-level* :(オプション) ログしきい値の重大度を設定します。
  - log-emerg : システムは使用できません。
  - log-alert : 即時のアクションが必要です。
  - log-crit : 危険な状態
  - log-err : エラー状態
  - log-warning : 警告状態
  - log-notice : 正常だが重要な状態 (デフォルト)
  - log-info : 情報メッセージ
  - log-debug : デバッグ メッセージ
- vrf {management | *vrf-name*} :(オプション) 管理 VRF インスタンスまたは設定済み VRF インスタンスのログ サーバーを構成します。

X.509v3 PKI 証明書の構成の詳細については、『*Dell EMC SmartFabric OS10 ユーザー ガイド*』を参照してください。

[監査ログの有効化]

[論拠]: スイッチでのユーザー アクティビティーと構成の変更を監視するには、監査ログを有効にします。sysadmin と secadmin の役割でのみ、監査ログの有効化、表示、クリアを行うことができます。

[構成]:

- 監査ログを構成します。

  ```
  OS10(config)# logging audit enable
  OS10(config)# exit
  OS10# write memory
  ```

- 監査ログを表示します。

  ```
  show logging audit [reverse] [number]
  ```

  - reverse : エントリーを最新のイベントから表示します。
  - *number* : 指定した数の監査ログ エントリー ユーザーを 1 ~ 65535 の範囲で表示します。

[有効なログ ルールの表示]

```
OS10# show running-configuration logging
!
logging audit enable
```

NTP ルール

Network Time Protocol (NTP) は、分散タイム サーバーとクライアントのセットでの計時を同期し、大規模で多様なネットワーク内での時間分布を調整します。NTP クライアントは、正確に時間を測定する NTP サーバーと同期します。

[信頼できる NTP サーバーの構成]

[論拠]: 信頼できる NTP サーバーと時間を同期するようにシステムを構成します。

[構成]:

```
OS10(config)# ntp server ntp1-server-ip-address
OS10(config)# exit
OS10# write memory
```

ntp1-server-ip-address : NTP サーバーの IPv4 アドレスを A.B.C.D 形式で入力するか、IPv6 アドレスを A::B 形式で入力します。

[信頼できるセカンダリー NTP サーバーの構成]

[論拠]: 信頼できるセカンダリー NTP サーバーと時間を同期するようにシステムを構成します。

[構成]:

```
OS10(config)# ntp server ntp2-server-ip-address
OS10(config)# exit
OS10# write memory
```

ntp1-server-ip-address : NTP サーバーの IPv4 アドレスを A.B.C.D 形式で入力するか、IPv6 アドレスを A::B 形式で入力します。

[NTP 認証の構成]

[論拠]: NTP 認証とそれに対応する信頼できるキーは、信頼できるタイム ソースを持つ NTP パケットの信頼性の高い交換を可能にします。NTP 認証では、メッセージ ダイジェスト 5 (MD5) アルゴリズムが使用されます。キーは、NTP タイム ソースに送信される同期パケットに組み込まれています。

[構成]:

```
OS10(config)# ntp authentication-key number {sha1 | sha2-256} key
OS10(config)# ntp master {2-10}
OS10(config)# exit
OS10# write memory
```

- *number* : 認証キー番号を 1 ~ 4294967295 の範囲で入力します。
- `sha1` : SHA1 暗号化を使用するように設定します。
- `sha2-256` : sha2-256 暗号化を使用するように設定します。

[使用されている NTP 認証の表示]

システムで構成されている NTP 認証を表示するには、次のようにします。

```
OS10# show running-configuration ntp
!
ntp authenticate
ntp authentication-key 345 md5 0 5A60910FED211F02
ntp server 1.1.1.1 key 345
ntp trusted-key 345
ntp master 7
...
```

ループバック ルール

ループバック インターフェイスは仮想インターフェイスです。物理インターフェイスとは異なり、ループバック インターフェイスは手動で削除しない限りダウンしません。このプロパティは、デバイスの識別と安定性のためのセキュリティと整合性を提供します。

[ループバック インターフェイスの構成]

[論拠]: システムの複数のサービスで使用できるループバック インターフェイスを構成します。

[構成]:

```
OS10(config)# interface loopback 0
OS10(config)# exit
OS10# write memory
```

[複数のループバック インターフェイスの削除]

[論拠]: 複数のループバック インターフェイスが構成されていないことを確認します。

[構成]:

```
OS10(config)# no interface loopback loopback-instance
OS10(config)# exit
OS10# write memory
```

[AAA サービスのループバック インターフェイスへのバインド]

[論拠]: AAA サービスはループバック インターフェイスにバインドされるため、AAA サービスが中断されることはありません。

[構成]:

```
OS10(config)# ip tacacs source-interface loopback 0
OS10(config)# exit
OS10# write memory
```

[NTP サービスのループバック インターフェイスへのバインド]

[論拠]: NTP サービスはループバック インターフェイスにバインドされるため、AAA サービスが中断されることはありません。

[構成]:

```
OS10(config)# ntp source loopback 0
OS10(config)# exit
OS10# write memory
```

[コントロール プレーン ポリシーの構成]

[論拠]: コントロールプレーンの ACL を使用して、CPU に送信されるパケットを選択的に制限することにより、フラッディングや DoS 攻撃を回避できます。

[構成]:

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ip access-group acl_name in
OS10(config-control-plane)# end
OS10# write memory
```

メモ: コントロール プレーンに適用する前に、必要な ACL ルールを定義します。

データ プレーン ルール

データ プレーンは、ユーザーのトラフィックを伝送するネットワークの一部です。データ プレーン ルールには、ユーザー データに影響するサービスや設定が含まれます。内部ネットワークをインターネットなどの外部ネットワークに接続するボーダーフィルタリング デバイスに、これらのルールを適用します。

[外部ネットワークからのプライベート ソース アドレスの禁止]

[論拠]: プライベート IP アドレスは、ワークステーション、プリンター、DMZ などを接続するネットワークなどの内部ネットワークで使用することを目的としています。これらの IP アドレスは、パブリック IP アドレスを使用するインターネットにはルーティングされません。インターネットから送信されるプライベート IP アドレスは、ほとんどが攻撃を目的としています。内部ネットワーク上に存在する必要があるソース アドレスを持つ外部ネットワークからのトラフィックをすべて拒否するように ACL ルールを構成し、外部ネットワークに接続するインターフェイスに適用します。

注意: アドレス範囲をブロックする前に、マルチキャストが使用されていないことを確認します。

[構成]:

```
OS10(config)# ip access-list deny-private-external
OS10(config-ipv4-acl)# deny ip source-ip-address mask any log
OS10(config-ipv4-acl)# end
OS10# write memory
```

[アウトバウンド トラフィックでの外部ソース アドレスの禁止]

[論拠]: アウトバウンド トラフィックが、組織の IP アドレス範囲の有効な内部アドレスのみを使用していることを確認します。

[構成]:

```
OS10(config)# ip access-list deny-source-external
OS10(config-ipv4-acl)# permit ip internal-ip-address mask any
OS10(config-ipv4-acl)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip access-group deny-source-external in
OS10(conf-if-eth1/1/1)# end
OS10# write memory
```

ネイバー認証

ルーティング プロトコルに認証を使用すると、不正ユーザーがルーティング テーブルを破損するのを防ぐことができます。

[BGP を使用する場合の BGP 認証の構成]

[論拠]: BGP を構成し、両方の BGP ピアでパスワードを使用してセッションを保護します。2 個の BGP ピア間で MD5 認証を構成する場合、TCP 接続の各セグメントが検証され、TCP 接続で送信されるすべてのセグメントで MD5 ダイジェストがチェックされます。

[構成]:

```
OS10(conf-router-neighbor)# password {9 encrypted-password-string | password-string}
OS10(conf-router-neighbor)# end
OS10# write memory
```

- 9 *encrypted-password-string* : 9 と入力し、暗号化されたパスワードを入力します。
- *password-string* : 認証用のパスワードを入力します。最大 128 文字です。

[有効な BGP ネイバー認証の表示]

システムで有効になっている BGP ネイバー認証を表示するには、次のようにします。

```
OS10# show running-configuration bgp
!
router bgp 100
 !
 neighbor 1.1.1.1
  password 9 9ee88a6225a049667a2e5294d8b0808c2ac2141a2930c06e431bf40cfcf685b1
....
```

[OSPF を使用する場合の OSPF 認証の構成]

[論拠]: OSPF を構成し、両方の OSPF ピアでパスワードを使用してセッションを保護します。

[構成]:

```
OS10(conf-if-eth1/1/1)# ip ospf message-digest-key 2 md5 password
OS10(conf-if-eth1/1/1)# end
OS10# write memory
```

[有効な OSPF ネイバー認証の表示]

システムで有効になっている OSPF ネイバー認証を表示するには、次のようにします。

```
OS10# show running-configuration ospf
!
ip ospf 100 area 0.0.0.0
```

```
ip ospf message-digest-key 2 md5 sample12345
...
```

[プロキシ ARP の無効化]

[論拠]: プロキシ ARP は、ネットワークに存在しないデバイスの MAC アドレスを取得するために、他のデバイスの代わりにネットワーク デバイスが使用する技術です。ネットワーク デバイスが正しく構成されていないと、DoS 攻撃を受ける可能性があります。

[構成]:

```
OS10(config)# interface interface-name
OS10(conf-if-eth1/1/1)# no ip proxy-arp
OS10(conf-if-eth1/1/1)# end
OS10# write memory
```

X.509v3 証明書

OS10 は、スイッチとホスト (RADIUS サーバーなど) との間の通信を保護するために、X.509v3 証明書をサポートします。スイッチとサーバーの両方が、認証局 (CA) によって発行された署名済みの X.509v3 証明書の公開キーを交換して、相互に認証を行います。認証局は、プライベート キーを使用してホスト証明書に署名します。

証明書の署名リクエストとプライベート キーの生成

[論拠]: ネットワーク内の OS10 スイッチでのセキュアな通信とユーザー認証のために X.509v3 証明書を使用する場合、認証局 (CA) による公開鍵基盤 (PKI) が必要です。CA は、ネットワーク デバイスの信頼性を証明する証明書に署名します。

[構成]:

- EXEC モードでプライベート キーと CSR を作成します。CSR ファイルをホーム ディレクトリーまたはフラッシュ :に保存します。これにより、後で CA サーバーにコピーできるようになります。*キーパス*を指定して、ホーム ディレクトリーなどの安全で永続的な場所に *device.key* ファイルを保存するか、*プライベート* オプションを使用して、ユーザーに表示されない内部ファイル システムのプライベートな隠れた場所にキー ファイルを保存します。

  ```
  OS10# crypto cert generate request cert-file cert-path key-file {private | keypath}
  country 2-letter code state state locality city organization organization-name orgunit
  unit-name cname common-name email email-address validity days length length altname alt-
  name]
  ```

  - `request` : CA にコピーする証明書の署名リクエストを作成します。
  - `cert-file cert-path` :(オプション) 自己署名証明書または CSR が保存されているローカル パスを入力します。フル パスまたは相対パスを入力できます。例 : `flash://certs/s4810-001-request.csr` または `usb://s4810-001.crtcert-file` オプションを入力しない場合、システムにより、証明書の署名リクエストの残りのフィールドを入力するように求められます。`copy` コマンドを使用して、CSR を CA にエクスポートします。
  - `key-file {key-path | private}` : ダウンロードした、またはローカルに生成されたプライベート キーが保存されているローカル パスを入力します。キーがリモート サーバーにダウンロードされた場合は、HTTPS、SCP、SFTP などの安全な方法でサーバーのパスを入力します。`private` を入力して、キーをローカルの隠れた場所に保存します。
  - `country 2-letter-code` :(オプション) 国を識別する 2 文字のコードを入力します。
  - `state state` : 都道府県の名前を入力します。
  - `locality city` : 市町村の名前を入力します。
  - `organization organization-name` : 組織の名前を入力します。
  - `orgunit unit-name` : ユニットの名前を入力します。
  - `cname common-name` : 証明書に割り当てられた共通名を入力します。共通名は、デバイスを接続するために提示される主要な ID です。デフォルトでは、スイッチのホスト名に共通名が使用されます。スイッチに、IP アドレスなどの別の共通名を構成できます。*common-name* 値がデバイスの ID と一致しない場合、署名済み証明書は検証されません。
  - `email email-address` : 組織との通信に使用する有効な E メール アドレスを入力します。

- `validity days`：証明書の有効日数を入力します。CSR には有効性は関係ありません。自己署名証明書の場合、デフォルトは 3650 日または 10 年です。
- `length bit-length`：キーワードの長さのビット値を入力します。FIPS モードでは、値の範囲は 2048 ~ 4096 です。非 FIPS モードでは、値の範囲は 1024 ~ 4096 です。FIPS モードと非 FIPS モードのデフォルト キーの長さは 2048 ビットです。FIPS モードのキーの長さの最小値は 2048 ビットです。非 FIPS モードのキーの長さの最小値は 1024 ビットです。
- `altname altname`：組織の代替名を入力します。例えば、`altname IP:192.168.1.100` などの IP アドレスを使用できます。

- CSR を CA サーバーにコピーします。

```
OS10# copy home://DellHost.pem scp:///file-path/DellHost.pem
password:
```

CA サーバーは、プライベート キーを使用して CSR に署名します。CA サーバーは、OS10 スイッチが署名済み証明書をダウンロードしてインストールできるようにします。

- ホスト証明書をインストールします。
  - CA サーバーによって署名された X.509v3 証明書を、ローカルのホーム ディレクトリーに HTTPS、SCP、SFTP などの安全な方法でダウンロードするには、copy コマンドを使用します。
  - `crypto cert install` コマンドを使用して、証明書と、CSR によって生成されたプライベート キーをインストールします。

```
crypto cert install cert-file home://cert-filepath key-file {key-path | private}
[password passphrase] [fips]
```

[証明書の署名リクエストとプライベート キーの生成]

```
OS10# crypto cert generate request cert-file home://DellHost.pem key-file home://DellHost.key
email admin@dell.com length 1024 altname DNS:dell.domain.com
Processing certificate ...
Successfully created CSR file /home/admin/DellHost.pem and key
OS10# copy home://DellHost.pem scp:///tftpuser@10.11.178.103:/tftpboot/certs/DellHost.pem
password:
OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_host1_CA1.pem home://
Dell_host1_CA1.pem
password:
OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_host1_CA1.key home://
Dell_host1_CA1.key
password:
OS10# crypto cert install cert-file home://Dell_host1_CA1.pem key-file home://
Dell_host1_CA1.key
Processing certificate ...
Certificate and keys were successfully installed as "Dell_host1_CA1.pem" that may be used in
a
security profile. CN = Dell_host1_CA1
```

[信頼できる証明書の表示]

次の出力では、インストールされた証明書、有効期間、CA に関する詳細が表示されます。

```
OS10# show crypto cert
--------------------------------------
| Installed non-FIPS certificates |
--------------------------------------
Dell_host1_CA1.pem
--------------------------------------
| Installed FIPS certificates |
--------------------------------------

OS10# show crypto cert Dell_host1_CA1.pem
------------ Non FIPS certificate -----------------
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4096 (0x1000)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = California, O = Dell EMC, OU = Networking, CN = Dell_interCA1
Validity
Not Before: Jul 25 19:11:19 2018 GMT
```

```
Not After : Jul 22 19:11:19 2028 GMT
Subject: C = US, ST = California, L = Santa Clara, O = Dell EMC, OU = Networking, CN
= Dell_host1_CA1
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:e7:81:4b:4a:12:8d:ce:88:e6:73:3f:da:19:03:
c6:56:01:19:b2:02:61:3f:5b:1e:33:28:a1:ed:e3:
85:bc:56:fb:18:d5:16:2e:a0:e7:3a:f9:34:b4:df:
37:97:93:a9:b9:94:b2:9f:69:af:fa:31:77:68:06:
89:7b:6d:fc:91:14:4a:c8:7b:23:93:f5:44:5a:0a:
3f:ce:9b:af:a6:9b:49:29:fd:fd:cb:34:40:c4:02:
30:95:37:28:50:d8:81:fb:1f:83:88:d9:1f:a3:0e:
49:a1:b3:df:90:15:d4:98:2b:b2:38:98:6e:04:aa:
bd:92:1b:98:48:4d:08:49:69:41:4e:6a:ee:63:d8:
2a:9f:e6:15:e2:1d:c3:89:f5:f0:d0:fb:c1:9c:46:
92:a9:37:b9:2f:a0:73:cf:e7:d1:88:96:b8:4a:84:
91:83:8c:f0:9a:e0:8c:6e:7a:fa:6e:7e:99:3a:c3:
2c:04:f9:06:8e:05:21:5f:aa:6e:9f:b7:10:37:29:
0c:03:14:a0:9d:73:1f:95:41:39:9b:96:30:9d:0a:
cb:d0:65:c3:59:23:01:f7:f5:3a:33:b9:e9:95:11:
0c:51:f4:e9:1e:a5:9d:f7:95:84:9c:25:74:0c:21:
4f:8b:07:29:2f:e3:47:14:50:8b:03:c1:fb:83:85:
dc:bb
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Cert Type:
SSL Client, S/MIME
Netscape Comment:
OpenSSL Generated Client Certificate
X509v3 Subject Key Identifier:
4A:20:AA:E1:69:BF:BE:C5:66:2E:22:71:70:B4:7E:32:6F:E0:05:28
X509v3 Authority Key Identifier:
keyid:A3:39:CB:C7:76:86:3B:05:44:34:C2:6F:90:73:1F:5F:64:55:5C:76
X509v3 Key Usage: critical
```

自己署名証明書の生成

[論拠]: 管理者は、ネットワークに認証局を設置して証明書の信頼モデルを実装することは希望しないものの、トランスポート レイヤー セキュリティ (TLS) プロトコルが提供するプライバシー機能を利用したいと考える場合があります。この場合、自己署名証明書を使用できます。

自己署名証明書は CA によって署名されていません。スイッチは証明書の中で、自身を信頼できるデバイスとします。クライアントを接続すると、構成に応じて、ユーザーに証明書を信頼するように促す (例えば、Web ブラウザーでサイトが安全でないことを示す警告が表示された場合)、または証明書を拒否するよう促すプロンプトが表示されます。自己署名証明書では、中間者攻撃に対して保護されません。

[構成]:

1. EXEC モードで自己署名証明書を作成します。NVRAM などの安全で永続的な場所に `device.key` ファイルを保存します。

```
crypto cert generate self-signed [cert-file cert-path key-file {private | keypath}]
[country 2-letter code] [state state] [locality city] [organization organization-name]
[orgunit unit-name] [cname common-name] [email email-address] [validity days] [length
length] [altname alt-name]
```

「cert-file」オプションを入力する場合は、証明書とプライベート キーが保存されているローカル パスなど、必要なすべてのパラメーターを入力する必要があります。「cert-file」オプションを指定すると、証明書の他のパラメーター値の入力を求めるプロンプトが表示されます。例えば次のとおりです。

```
You are about to be asked to enter information that will be incorporated in your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value; if you enter '.', the field will be left
blank.
Country Name (2 letter code) [US]:
```

```
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) []:Starfleet Command
Organizational Unit Name (eg, section) []:NCC-1701A
Common Name (eg, YOUR name) [hostname]:S4148-001
Email Address []:scotty@starfleet.com
```

2. EXEC モードで自己署名証明書とキー ファイルをインストールします。

```
crypto cert install cert-file home://cert-filename key-file {key-path | private} [password
passphrase] [fips]
```

- `cert-file` *cert-path* ダウンロードした証明書のソースの場所を指定します。例：`home://s4048-001-cert.pem or usb://s4048-001-cert.pem`
- `key-file {`*key-path* `| private}` ダウンロードしたプライベート キーまたはローカルに生成されたプライベート キーを取得するローカル パスを指定します。プライベートを入力して、ローカルの隠れた場所からキーをインストールし、キー ファイルの名前を証明書の名前に変更します。
- `password` *passphrase* パスワードを使用して生成されたプライベート キーを復号化するために使用するパスワードを指定します。

3. `fips` では、証明書キー ペアを FIPS 準拠としてインストールします。`fips` を入力して、RADIUS over TLS などの、FIPS 対応アプリケーションによって使用される証明書キー ペアをインストールします。`fips` を入力しない場合は、証明書キー ペアが非 FIPS 準拠のペアとして保存されます。

   メモ: 証明書キー ペアを FIPS 準拠として生成するかどうかを判断します。FIPS モード以外で、FIPS 準拠の証明書キー ペアを使用しないでください。

4. `crypto cert generate request` コマンドで `key-file` プライベート オプションを使用した後に `fips` を入力した場合、FIPS 準拠のプライベート キーが内部ファイル システム内のユーザーには非表示の場所に保存されます。

証明書のインストールが正常に行われた場合、自己署名証明書のファイル名とその共通名が表示されます。`crypto security-profile` コマンドを使用してセキュリティ プロファイルの証明書を構成するには、ファイル名を使用します。

[例：自己署名証明書とキーの生成とインストール]

```
OS10# crypto cert generate self-signed cert-file home://DellHost.pem key-file home://
DellHost.key email admin@dell.com length 1024 altname DNS:dell.domain.com validity 365
Processing certificate ...
Successfully created certificate file /home/admin/DellHost.pem and key
OS10# crypto cert install cert-file home://DellHost.pem key-file home://DellHost.key
Processing certificate ...
Certificate and keys were successfully installed as "DellHost.pem" that may be used in a
security profile. CN = DellHost.
```

[自己署名証明書の表示]

```
OS10# show crypto cert
--------------------------------------
| Installed non-FIPS certificates |
--------------------------------------
DellHost.pem
--------------------------------------
| Installed FIPS certificates |
--------------------------------------
OS10# show crypto cert DellHost.pem
------------ Non FIPS certificate -----------------
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 245 (0xf5)
Signature Algorithm: sha256WithRSAEncryption
Issuer: emailAddress = admin@dell.com
Validity
Not Before: Feb 11 20:10:12 2019 GMT
Not After : Feb 11 20:10:12 2020 GMT
Subject: emailAddress = admin@dell.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:c7:12:ca:a8:d6:d2:1c:ab:66:9a:d1:db:50:5a:
b5:8a:e4:53:9d:f6:b4:fc:cd:f4:b9:46:8a:03:86:
be:0b:50:51:c7:25:76:9f:ff:b4:f9:f8:d9:6f:5d:
```

```
53:52:0c:4d:05:ed:31:23:79:44:5c:d7:62:01:9d:
41:e8:ff:3a:b0:35:0c:22:d7:ef:df:05:9a:28:6b:
95:10:8e:bc:c6:62:3a:82:30:0f:4f:4e:19:17:48:
f1:bd:1e:0c:4f:54:03:42:f3:a7:de:22:40:3d:5e:
6b:b2:8e:23:17:53:ef:10:d9:ae:1d:1f:d6:e4:ae:
25:9f:d9:39:60:5c:49:b0:ad
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
DA:39:A3:EE:5E:6B:4B:0D:32:55:BF:EF:95:60:18:90:AF:D8:07:09
X509v3 Subject Alternative Name:
DNS:dell.domain.com
Signature Algorithm: sha256WithRSAEncryption
b8:83:ae:34:bb:84:e6:b4:a3:fd:77:20:67:15:3f:02:76:ca:
f6:74:d4:d2:36:0e:58:8c:96:13:c2:85:8a:df:ba:c0:d9:c8:
```

証明書の失効

[論拠]: 証明書失効リスト (CRL) は、発行元である認証局 (CA) が予定された有効期限前に失効させたデジタル証明書のリストです。これらの証明書は、信頼できるものではなくなりました。

スイッチと外部デバイス (RADIUS や TLS サーバーなど) を接続する前に、CA 署名付き証明書を互いに提示して安全な接続を設定します。証明書の検証によりピアは互いの ID を認証でき、その後、証明書が発行元の CA によって失効されていないことを確認します。

証明書には、その証明書を発行した証明書配布ポイント (CDP) に関する URL やその他の情報が含まれています。URL を使用して、OS10 は証明書失効リスト (CRL) をダウンロードするために CDP にアクセスします。外部デバイスの証明書がリストにある場合、または CDP サーバーが応答しない場合、接続は設定されません。

[構成]:

1. 証明書配布ポイントの URL を EXEC モードで構成します。

   ```
   OS10# crypto cdp add cdp-name cdp-url
   ```

   スイッチによりアクセスされた CDP を EXEC モードで確認します。

   ```
   OS10# show crypto cdp [cdp-name]
   ```

   インストールされている CDP を削除するには、`crypto cdp delete cdp-name` コマンドを使用します。
2. CDP からダウンロードされた CRL を EXEC モードでインストールします。

   ```
   OS10# crypto crl install crl-path [crl-filename]
   ```

   スイッチにインストールされている CRL のリストを EXEC モードで表示します。

   ```
   OS10# show crypto crl [crl-filename]
   ```

   `crypto crl install` コマンドを使用して構成された手動でインストールされた CRL を削除するには、`crypto crl delete [crl-filename]`コマンドを使用します。

[例 : CDP の構成]

```
OS10# crypto cdp add cert1_cdp http://crl.chambersign.org/chambersignroot.crl
Successfully added CDP
OS10# show crypto cdp
---------------------------------------
| Manually installed CDPs |
---------------------------------------
cert1_cdp.crl_url
---------------------------------------
| Automatically installed CDPs |
---------------------------------------
```

[例 : CRL のインストール]

```
OS10# crypto crl install home://pki-regression/Network_Solutions_Certificate_
Authority.0.crl.pem
```

```
Processing file ...
issuer=C=US,O=Network Solutions L.L.C.,CN=Network Solutions Certificate Authority.0.crl.pem
lastUpdate=Jul 7 04:15:08 2019 GMT
nextUpdate=Jul 11 04:15:08 2019 GMT
OS10# show crypto crl
--------------------------------------
| Manually installed CRLs |
--------------------------------------
Network_Solutions_Certificate_Authority.0.crl.pem
--------------------------------------
| Downloaded CRLs |
--------------------------------------
```

[失効した証明書の表示]

次に、失効した証明書のリストを表示します。

```
OS10# show crypto crl COMODO_Certification_Authority.0.crl.pem
Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: sha1WithRSAEncryption
Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/
CN=COMODO Certification
Authority
Last Update: May 8 20:34:21 2019 GMT
Next Update: May 12 20:34:21 2019 GMT
CRL extensions:
X509v3 Authority Key Identifier:
keyid:0B:58:E5:8B:C6:4C:15:37:A4:40:A9:30:A9:21:BE:47:36:5A:56:FF
X509v3 CRL Number:
2904
No Revoked Certificates.
Signature Algorithm: sha1WithRSAEncryption
5b:77:52:c0:a0:4e:77:be:4a:c4:6a:7e:92:98:2e:a1:6b:3c:
ad:2d:ac:db:0a:19:1d:a3:56:98:7f:d6:93:f3:1d:4b:61:40:
c3:e0:40:45:0b:41:4b:66:87:35:2b:3a:4c:f3:f1:7e:44:7e:
fe:7f:51:5d:17:ee:b3:4c:15:75:a6:a0:7b:2e:b1:92:3e:b6:
71:a8:01:8d:78:ac:80:3b:16:f2:f1:a8:fd:09:68:9f:7e:09:
55:c6:80:2c:2f:e7:f3:54:51:94:3a:d8:b4:d6:00:3f:63:b1:
19:f3:42:2a:d2:c4:3b:de:c4:4d:ad:f0:72:c5:b4:25:51:e5:
3c:76:8b:97:3c:db:fe:3f:7f:41:d2:d9:aa:7f:98:90:6b:cf:
27:53:0e:66:83:8e:cc:81:ef:6a:e5:cd:c2:f1:e2:ea:84:4f:
73:bb:90:5a:b3:19:a3:50:6a:c7:b3:99:e4:09:fd:56:99:83:
3a:15:93:b0:4a:49:28:78:69:85:de:fc:06:cc:b9:a5:5b:d9:
4a:b0:46:90:ce:94:3a:9c:f3:04:e4:d7:98:36:29:a8:8b:fe:
72:26:b0:fd:39:5e:14:f5:00:6d:0e:4f:ec:d4:a5:ca:4f:e1:
d9:4f:5a:37:21:e3:a2:fb:80:db:cd:68:0b:a0:fa:58:0d:5e:
40:e1:e4:1c
```

セキュリティ プロファイルの構成

さまざまな OS10 アプリケーションで個別のセキュリティ認証情報を使用するには、複数のセキュリティ プロファイルを構成し、OS10 アプリケーションに割り当てることができます。セキュリティ プロファイルは、証明書とプライベート キーのペアで構成されています。

例えば、RADIUS over TLS 認証と SmartFabric サービスのために、異なるセキュリティ プロファイルを維持できます。プロファイルを構成するときに、アプリケーションにセキュリティ プロファイルを割り当てます。

証明書キー ペアをインストールする場合、どちらも証明書の名前を使用します。例えば、次のように証明書をインストールします。

```
OS10# crypto cert install cert-file home://Dell_host1.pem key-file home://abcd.key
```

証明書キー ペアは、`Dell_host1.pem` および `Dell_host1.key` としてインストールされます。構成コマンドで、`Dell_host1` としてペアを入力します。セキュリティ プロファイルを構成する場合は、`certificate certificate-name` コマンドに `Dell_host1` と入力します。

- CONFIGURATION モードでアプリケーション固有のセキュリティ プロファイルを作成します。

```
OS10(config)# crypto security-profile profile-name
```

- 証明書とプライベート キーのペアを SECURITY-PROFILE モードでセキュリティ プロファイルに割り当てます。`certificate-name` には、`show crypto certs` 出力に表示される証明書キー ペアの名前を `.pem` 拡張子なしで入力します。

```
OS10(config-sec-profile)# certificate certificate-name
exit
```

- (オプション) SECURITY-PROFILE モードで外部デバイスから受信した証明書の CRL チェックを有効にします。CRL チェックでは、スイッチにインストールされている CRL を使用して証明書の有効性を確認します。

```
OS10(config-sec-profile)#revocation-check
```

- (オプション) SECURITY-PROFILE モードで、外部デバイスによって提供される証明書に対してピア名のチェックを有効にします。ピア名のチェックにより、証明書がリモート サーバー名などのピア デバイス名と一致することを確認します。

```
OS10(config-sec-profile)#peer-name-check
```

- セキュリティ プロファイルを使用して、X.509v3 ベースのサービスを構成します。例えば、X.509v3 証明書を使用して RADIUS over TLS 認証を構成するには、`radius-server host tls` コマンドを入力します。

```
OS10(config)# radius-server host {hostname | ip-address} tls security-profile profile-name
[auth-port port-number] key {0 authentication-key | 9 authentication-key |
authenticationkey}
```

[例：RADIUS over TLS 認証のセキュリティ プロファイル]

```
OS10# show crypto cert
--------------------------------------
| Installed non-FIPS certificates |
--------------------------------------
dv-fedgov-s6010-1.pem
--------------------------------------
| Installed FIPS certificates |
--------------------------------------
OS10#
OS10(config)#
OS10(config)# crypto security-profile radius-prof
OS10(config-sec-profile)# certificate dv-fedgov-s6010-1
OS10(config-sec-profile)# revocation-check
OS10(config-sec-profile)# peer-name-check
OS10(config-sec-profile)# exit
OS10(config)#
OS10(config)# radius-server host radius-server-2.test.com tls security-profile radius-prof
key radsec
OS10(config)# end
OS10# show running-configuration crypto security-profile
!
crypto security-profile radius-prof
   certificate dv-fedgov-s6010-1
```

[セキュリティ プロファイルが有効化されているかどうかのチェック]

セキュリティ プロファイルが有効化されているかどうかは次のように示されます。

```
OS10# show running-configuration radius-server
radius-server host radius-server-2.test.com tls security-profile radius-prof key 9
2b9799adc767c0efe8987a694969b1384c541414ba18a44cd9b25fc00ff180e9
```

SSH のスマート カード認証

OS10 では、SSH を使用してデバイスに接続する際のユーザー認証に、共通アクセス カード (CAC) や個人識別情報の検証 (PIV) スマート カードを使用できます。CAC および PIV スマート カードには、認証局によって発行された公開鍵基盤 (PKI) X.509v3 証明書が含まれています。この機能を使用すると、OS10 ソフトウェアによってユーザー認証、E メール署名、および暗号化を検証できます。スマート カード認証を使用するには、X.509v3 認証をサポートしている SSH クライアントを使用します。

[論拠] : ユーザーは強力で複雑なパスワードを使用してデバイスに安全にアクセスすることができますが、ユーザーはパスワードを書き留めたり、安全でない場所に保管したりする傾向があります。SSH にスマート カードを使用すると、セキュリティが強化され、ユーザーは複雑なパスワードを記憶する必要がなくなります。

OS10 SSH サーバーにより、パスワードありとなしの 2 種類の形式で X.509v3 スマート カード認証がサポートされます。パスワードを使用して X.509v3 認証を使用する場合、RADIUS または TACACS+認証を使用したリモート認証とともに、X.509v3 認証を使用できます。

[パスワードを使用したリモート ユーザー認証]

X.509v3 SSH 認証、および RADIUS または TACACS+を使用したリモート認証を行うようにスイッチを構成する場合、SSH を使用して接続すると、次のシーケンスが発生します。

1. システムまたはキーボードのカード リーダー スロットに、CAC または PIV スマート カードを挿入します。
2. RFC 6187 X.509v3 互換 SSH クライアント アプリケーションを起動して、認証をスマート カードまたは CAC に設定し、OS10 スイッチへの接続を確立します。
3. SSH クライアント アプリケーションは、スイッチへの初期接続を確立し、X.509v3 認証をネゴシエートして、OS10 スイッチ X.509v3 証明書を検証します。
4. SSH クライアント アプリケーションによって、CAC または PIV カードから必要な認証証明書を選択するよう促されます。
5. SSH クライアント アプリケーションによって、CAC または PIV カードの PIN の入力を求めるプロンプトが表示されます。
6. SSH クライアント アプリケーションにより、X.509v3 証明書を使用して認証リクエストが送信されます。
7. OS10 SSH サーバーは、公開証明書を検証します。これには、信頼できるチェーン、有効な日付範囲、使用状況フィールドの検証が含まれます。フィールドのいずれかが無効な場合、認証は失敗します。
8. 構成された OS10 セキュリティ プロファイルが失効チェックを要求すると、OS10 SSH サーバーは証明書が失効していないことを確認します。検証は、適切な CRL を確認するか、OCSP リクエストを適切な OCSP レスポンダーに送信することによって行われます。
9. 証明書が失効している場合、認証は失敗します。
10. セキュリティ プロファイルでピア名のチェックが有効化されている場合、OS10 SSH サーバーは、ユーザー証明書の共通名またはプリンシパル名フィールドをユーザー名と照合します。一致しない場合、認証は失敗します。
11. OS10 SSH サーバーからパスワードの入力を求められます。
12. OS10 SSH サーバーは、ユーザー名と返されたパスワードを使用して、標準 RADIUS または TACACS+ユーザー認証を実行します。
13. 認証に成功すると、SSH セッションが続行されます。

[パスワードを使用したローカル ユーザー認証]

OS10 SSH サーバーを X.509v3 SSH ローカル認証に構成し、SSH を使用して接続すると、次のシーケンスが発生します。

1. PC またはキーボードのカード リーダー スロットに、CAC または PIV スマート カードを挿入します。
2. RFC 6187 X.509v3 互換 SSH クライアント アプリケーションを起動して、認証をスマート カードまたは CAC に設定し、OS10 スイッチへの接続を確立します。
3. SSH クライアント アプリケーションは、スイッチへの初期接続を確立し、X.509v3 認証をネゴシエートして、X.509v3 証明書を検証します。
4. SSH クライアント アプリケーションによって、CAC または PIV カードから必要な認証証明書を選択するよう促されます。
5. SSH クライアント アプリケーションによって、CAC または PIV カードの PIN の入力を求めるプロンプトが表示されます。
6. SSH クライアントアプリケーションにより、X.509v3 証明書を使用して認証リクエストが送信されます。
7. OS10 SSH サーバーは、公開証明書を検証します。これには、信頼できるチェーン、有効な日付範囲、使用状況フィールドの検証が含まれます。フィールドのいずれかが無効な場合、認証は失敗します。
8. 構成された OS10 セキュリティ プロファイルが失効チェックを要求すると、OS10 SSH サーバーは証明書が失効していないことを確認します。検証は、適切な CRL を確認するか、OCSP リクエストを適切な OCSP レスポンダーに送信することによって行われます。
9. 証明書が失効している場合、認証は失敗します。
10. セキュリティ プロファイルでピア名のチェックが有効化されている場合、OS10 SSH サーバーは、ユーザー証明書の共通名またはプリンシパル名フィールドをユーザー名と照合します。
11. 一致しない場合、OS10 SSH サーバーは、ユーザー証明書フィールドを、そのローカル ユーザー名に対して構成されたすべての証明書と照合しようとします。
12. 一致しない場合、認証は失敗します。
13. OS10 SSH サーバーからパスワードの入力を求められます。
14. OS10 SSH サーバーは、ユーザー名と返されたパスワードを使用して、標準のローカル ユーザー認証を実行します。
15. 認証に成功すると、SSH セッションが続行されます。

[パスワードなしのローカル ユーザー認証]

OS10 SSH サーバーを X.509v3 SSH のローカル認証に構成し、SSH を使用して接続すると、次のシーケンスが発生します。

1. PC またはキーボードのカード リーダー スロットに、CAC または PIV スマート カードを挿入します。

2. RFC 6187 X.509v3 互換 SSH クライアント アプリケーションを起動して、認証をスマート カードまたは CAC に設定し、OS10 スイッチへの接続を確立します。
3. SSH クライアント アプリケーションは、スイッチへの初期接続を確立し、X.509v3 認証をネゴシエートして、OS10 スイッチ X.509v3 証明書を検証します。
4. SSH クライアント アプリケーションによって、CAC または PIV カードから必要な認証証明書を選択するよう促されます。
5. SSH クライアント アプリケーションによって、CAC または PIV カードの PIN の入力を求めるプロンプトが表示されます。
6. SSH クライアントアプリケーションにより、X.509v3 証明書を使用して認証リクエストが送信されます。
7. OS10 SSH サーバーは、公開証明書を検証します。これには、信頼できるチェーン、有効な日付範囲、使用状況フィールドの検証が含まれます。フィールドのいずれかが無効な場合、認証は失敗します。
8. 構成された OS10 セキュリティ プロファイルが失効チェックを要求すると、OS10 SSH サーバーは証明書が失効していないことを確認します。検証は、適切な CRL を確認するか、OCSP リクエストを適切な OCSP レスポンダーに送信することによって行われます。
9. 証明書が失効している場合、認証は失敗します。
10. OS10 SSH サーバーは、ユーザー証明書フィールドを、そのローカル ユーザー名に対して構成された証明書と照合しようとします。
11. 一致する場合は認証が成功し、SSH セッションはパスワード プロンプトなしで続行されます。

[パスワードを使用したリモート ユーザー認証の構成]

スマート カードおよびパスワードによるリモート ユーザー認証をサポートするには、次のように構成します。

- RADIUS または TACACS+認証を有効にします。

```
radius-server host {hostname | ip-address} key {0 authentication-key | 9 authentication-
key | authentication-key} [auth-port port-number]
aaa authentication login default group radius local
```

- SSH サーバーで、X.509v3 認証を有効にします。

```
ip ssh server x509v3-authentication security-profile profile-name
```

- すべての SSH ログイン試行で X.509v3 証明書が必要な場合は、SSH サーバーで、プレーン パスワード認証と SSH 公開キー認証を無効にします。

```
no ip ssh server password-authentication
no ip ssh server pubkey-authentication
```

[パスワードを使用したローカル ユーザー認証の構成]

スマート カードおよびパスワードによるローカル ユーザーの認証をサポートするには、次のように構成します。

- SSH サーバーで、X.509v3 認証を有効にします。

```
ip ssh server x509v3-authentication security-profile profile-name
```

- すべての SSH ログイン試行で X.509v3 証明書が提示される場合は、SSH サーバーで、プレーン パスワード認証と SSH 公開キー認証を無効にします。

```
no ip ssh server password-authentication
no ip ssh server pubkey-authentication
```

- セキュリティ プロファイルでキー使用率のチェックを有効にしていても、ユーザーの証明書でユーザーのログイン名とは異なる名前の構文を使用している場合は、ユーザー証明書の詳細を構成して、SSH サーバーがユーザーの証明書をアカウントと照合できるようにします。

```
username username certificate subject “x509v3-subject-string”
or
username username certificate principal-name user-principal-name-string
or
username username certificate fingerprint fingerprint-value
```

[パスワードなしのローカル ユーザー認証の構成]

スマート カードとパスワードを使用したパスワードレスのローカル ユーザー認証をサポートするには、次のように構成します。

- SSH サーバーで、パスワードレス X.509v3 認証を有効にします。

```
ip ssh server x509v3-authentication security-profile profile-name password-less
```

- 証明書が構成されていないユーザーのために、プレーン パスワード認証を有効のままにしておきます。

```
ip ssh server password-authentication
```

- ユーザーが SSH 公開キーのパスワードレス認証を代わりに使用する必要がある場合は、プレーン公開キー認証を有効のままにしておいてください。

```
ip ssh server pubkey-authentication
```

- ユーザーの X.509v3 証明書の詳細を構成して、SSH サーバーがユーザーの証明書をアカウントと照合できるようにします。

```
username username certificate subject “x509v3-subject-string”
or
username username certificate principal-name user-principal-name-string
or
username username certificate fingerprint fingerprint-value
```

フル スイッチ モードの OS10 10.4.3.0 以降のリリースでの新しいセキュリティ証明書の生成とインストール

[論拠]: VLT または SmartFabric サービスが有効になっていて、OS 10.5.0.7P3 およびそれ以前のサポートされているリリースが実行されているスイッチでは、安全なチャネルを使用して相互に通信します。安全なチャネルを確立するために、OS10 は X.509v3 証明書を使用します。

ユーザーがシステムにログ インすると、10.4.3.x から 10.5.0.7P3 の OS10 イメージにより、クラスター マネージャーがデフォルトの認証情報を使用しているという警告メッセージが表示されます。

[構成に関するメモ：]

- OS10 を再インストールした場合でも、証明書はシステム上に存在しています。OS10 を再インストールする場合は、`no cluster security-profile` コマンドおよび `cluster security-profile` *`profile-name`* コマンドを使用して、セキュリティ プロファイルの削除と再追加をしてから、証明書を再インストールします。

次の手順で有効な証明書をインストールすると、警告メッセージの表示がなくなり、システムが正常に機能するようになります。この手順は、OS10 リリース 10.4.3.0 以降でのみ機能します。OS10 の 10.4.1.4 から 10.4.2.x のリリースを実行している場合は、それ以降のリリースにアップグレードしてください。

[構成]:

1. 両方のデバイスで、OS10 のバージョンを確認します。

   [スイッチ A：]

```
Switch-A# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved. OS Version: 10.5.0.7P3
Build Version: 10.5.0.7.745
Build Time: 2020-06-02T22:46:24+0000
System Type: MX9116N-ON
Architecture: x86_64
Up Time: 00:07:32
```

   [スイッチ B：]

```
Switch-B# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved. OS Version: 10.5.0.7P3
Build Version: 10.5.0.7.745
Build Time: 2020-06-02T22:46:24+0000
System Type: MX9116N-ON
Architecture: x86_64
Up Time: 00:08:10
```

2. システムがフル スイッチ モードであることを確認します。

   [スイッチ A：]

```
Switch-A# show switch-operating-mode
8713-ToR-2# Switch-Operating-Mode : Full Switch Mode
```

[スイッチ B :]

```
Switch-B# show switch-operating-mode
8713-ToR-2# Switch-Operating-Mode : Full Switch Mode
```

3. VLT が収束していることを確認します。

[スイッチ A :]

```
Switch-A# show vlt 255
Domain ID : 255
Unit ID : 1 Role : primary
Version : 2.3
Local System MAC address : 20:04:0f:20:86:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::1
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
------------------------------------------------------------------------------
2 20:04:0f:21:9a:00 up fda5:74c8:b79e:1::2 2.3
```

[スイッチ B :]

```
Switch-B# show vlt 255
Domain ID : 255
Unit ID : 2 Role : secondary
Version : 2.3
Local System MAC address : 20:04:0f:21:9a:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::2
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
------------------------------------------------------------------------------
1 20:04:0f:20:86:00 up fda5:74c8:b79e:1::1 2.3
```

4. OS10 CLI を使用して自己署名証明書を作成します。これは、同じ VLT ドメインまたは SmartFabric クラスター内のいずれかのスイッチで行うことができます。

[スイッチ A :]

```
Switch-A# crypto cert generate self-signed cert-file home://dell.crt key-file home://
dell.ky cname sfscert
Processing file ...
Successfully created certificate file and key
```

また、次のパラメーターを指定することもできます。

- `country` *`2-letter-code`* :(オプション) 国を識別する 2 文字のコードを入力します。
- `state` *`state`* : 都道府県の名前を入力します。
- `locality` *`city`* : 市町村の名前を入力します。
- `organization` *`organization-name`* : 組織の名前を入力します。
- `orgunit` *`unit-name`* : ユニットの名前を入力します。
- `cname` *`common-name`* : 証明書に割り当てられた共通名を入力します。共通名は、デバイスを接続するために提示される主要な ID です。デフォルトでは、スイッチのホスト名に共通名が使用されます。スイッチに、IP アドレスなどの別の共通名を構成できます。*`common-name`* 値がデバイスの提示 ID と一致しない場合、署名済み証明書は検証されません。
- `email` *`email-address`* : 組織との通信に使用する有効な E メール アドレスを入力します。

- `validity days` ：証明書の有効日数を入力します。自己署名証明書の場合、デフォルトは 3650 日です。
- `length bit-length` ：キーワードの長さのビット値を入力します。FIPS モードでは、値の範囲は 2048 ~ 4096 です。非 FIPS モードでは、値の範囲は 1024 ~ 4096 です。FIPS モードと非 FIPS モードのデフォルト キーの長さは 2048 ビットです。FIPS モードのキーの長さの最小値は 2048 ビットです。非 FIPS モードのキーの長さの最小値は 1024 ビットです。
- `altname altname` ：組織の代替名を入力します。例えば、`altname IP:192.168.1.100` などの IP アドレスを使用できます。

5. 新しく作成された証明書がホーム ディレクトリーに存在するかどうかを確認します。

   [スイッチ A：]

```
Switch-A# dir home
Directory contents for folder: home
Date (modified) Size (bytes) Name
-------------------- ------------ --------------------------------------
2020-12-18T14:20:32Z 1017 dell.crt 2020-12-18T14:20:32Z 1675 dell.ky
```

6. 証明書とキーをスイッチ A から SCP サーバーにコピーします。この例では SCP が使用されていますが、TFTP または FTP サーバーを使用することもできます。

   [スイッチ A：]

```
Switch-A# copy home://dell.crt scp://<username>:<password>@100.104.54.214/dell.crt
Switch-A# copy home://dell.ky scp://<username>:<password>@100.104.54.214/dell.ky
```

7. 証明書とキーを SCP サーバーからスイッチ B にコピーします。

   [スイッチ B：]

```
Switch-B# copy scp://<username>:<password>@100.104.54.214/dell.crt home://dell.crt
Switch-B# copy scp://<username>:<password>@100.104.54.214/dell.ky home://dell.ky
```

   メモ: SFS クラスターまたは VLT ドメイン内のすべてのデバイスは、同じ証明書とキー ファイルを有している必要があります。

8. 証明書がスイッチ B にコピーされたかどうかを確認します。

   [スイッチ B：]

```
Switch-B# dir home
Directory contents for folder: home
Date (modified) Size (bytes) Name
-------------------- ------------ --------------------------------------
2020-12-18T14:59:51Z 1017 dell.crt 2020-12-18T15:00:42Z 1675 dell.ky
```

9. 自己署名証明書とキー ファイルをインストールします。

   [スイッチ A：]

```
Switch-A# crypto cert install cert-file home://dell.crt key-file home://dell.ky
```

   [スイッチ B：]

```
Switch-B# crypto cert install cert-file home://dell.crt key-file home://dell.ky
```

   `show crypto cert` コマンドを実行して、証明書がシステムにインストールされていることを確認します。

10. セキュリティ プロファイルを作成します。

    [スイッチ A：]

```
Switch-A(config)# crypto security-profile DELL123
```

    [スイッチ B：]

```
Switch-B(config)# crypto security-profile DELL123
```

11. 証明書とプライベート キーのペアをセキュリティ プロファイルに割り当てます。ファイル拡張子なしで証明書の名前を入力します。

[スイッチ A :]

```
Switch-A(config-sec-profile)# certificate dell
```

[スイッチ B :]

```
Switch-B(config-sec-profile)# certificate dell
```

12. クラスターのセキュリティ プロファイルを作成します。

[スイッチ A :]

```
Switch-A(config)# cluster security-profile DELL123
```

[スイッチ B :]

```
Switch-A(config)# cluster security-profile DELL123
```

13. (リリース 10.4.3.x を実行している場合のみ) 両方のデバイス上の/config/certs/ディレクトリーに `store` フォルダーを作成します。

```
Switch-A# system "sudo mkdir /config/certs/store"
```

```
Switch-B# system "sudo mkdir /config/certs/store"
```

14. 証明書を/config/certs/store/の場所にコピーし、両方の VLT ピアで `c_rehash` コマンドを実行します。

```
Switch-A# system "sudo cp /config/certs/dell.crt /config/certs/store/"
Switch-A# system "sudo c_rehash /config/certs/store/"
```

```
Switch-B# system "sudo cp /config/certs/dell.crt /config/certs/store/"
Switch-B# system "sudo c_rehash /config/certs/store/"
```

15. 新しい SSH セッションを開き、警告メッセージが表示されないことを確認します。新しい証明書が VLT ドメインまたは SFS クラスターで有効になっていない場合でも、システムは警告メッセージを生成しません。
16. MX デバイスの場合、マルチノード クラスター導入を実行しているなら、各 VLT ペアのいずれかの VLT ピアと、SFS プライマリー ノードを再起動します。MX 以外のデバイスの場合、VLTi リンクをフラップします。

注意: VLTi リンクをフラップしたり、ノードを再起動したりすると、一時的にパケット ロスが発生する場合があります。この手順は、メンテナンス ウィンドウで実行します。

17. (オプション) VLT が収束していることを確認します。

[スイッチ A :]

```
Switch-A# show vlt 255
Domain ID : 255
Unit ID : 1
Role : primary
Version : 2.3
Local System MAC address : 20:04:0f:20:86:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::1
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
------------------------------------------------------------------------------
2 20:04:0f:21:9a:00 up fda5:74c8:b79e:1::2 2.3
```

[スイッチ B :]

```
Switch-B# show vlt 255
Domain ID : 255
Unit ID : 2
Role : secondary
Version : 2.3
```

```
Local System MAC address : 20:04:0f:21:9a:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::2
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
--------------------------------------------------------------------------------
1 20:04:0f:20:86:00 up fda5:74c8:b79e:1::1 2.3
```