NetAppのハードウェアベースの暗号化の設定

ONTAP 9

NetApp
February 12, 2026

目次

NetAppのハードウェアベースの暗号化の設定

ONTAP ハードウェアベース暗号化について学ぶ

NetAppのハードウェアベースの暗号化は、データ書き込み時のFull Disk Encryption（FDE）をサポートします。ファームウェアに格納された暗号化キーがないとデータを読み取ることはできず、その暗号化キーには認証されたノードからしかアクセスできません。

NetAppのハードウェアベースの暗号化について

ノードは、外部キー管理サーバまたはオンボード キー マネージャから取得した認証キーを使用して自己暗号化ドライブへの認証を行います。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードにキーを提供します。外部キー管理サーバは、データとは別のストレージ システムで設定することを推奨します。
- オンボード キー マネージャは組み込みのツールで、データと同じストレージ システムからノードに認証キーを提供します。

NetApp Volume Encryptionをハードウェアベースの暗号化と組み合わせて使用すると、自己暗号化ドライブ上のデータを「二重に暗号化」できます。

自己暗号化ドライブを有効にすると、コア ダンプも暗号化されます。

> HAペアで暗号化SASまたはNVMeドライブ（SED、NSE、FIPS）を使用している場合は、システムを初期化（ブートオプション4または9）する前に、HAペア内のすべてのドライブについて、FIPSドライブまたはSEDを非保護モードに戻すのトピックの手順に従う必要があります。これを行わないと、ドライブを再利用した場合に将来データが失われる可能性があります。

サポートされている自己暗号化ドライブのタイプ

2種類の自己暗号化ドライブがサポートされています。

- 自己暗号化FIPS認定SASまたはNVMeドライブは、すべてのFASおよびAFFシステムでサポートされています。これらのドライブは「FIPSドライブ」と呼ばれ、連邦情報処理規格（FIPS）140-2レベル2の要件に準拠しています。認定機能により、暗号化に加えて、ドライブへのサービス拒否攻撃の防止など、保護機能も有効になります。FIPSドライブは、同じノードまたはHAペア上で他のタイプのドライブと混在させることはできません。
- ONTAP 9.6以降、AFF A800、A320、およびそれ以降のシステムでは、FIPSテストを受けていない自己暗号化NVMeドライブがサポートされます。これらのドライブは_SED_と呼ばれ、FIPSドライブと同じ暗号化機能を提供しますが、同じノードまたはHAペアで非暗号化ドライブと混在させることができます。
- すべてのFIPS準拠ドライブは、FIPS認定を受けたファームウェア暗号化モジュールを使用します。FIPSドライブの暗号化モジュールは、ドライブの外部で生成されたキーを使用しません（ドライブに入力された認証パスフレーズを使用してキー暗号化キーを取得します）。

> 非暗号化ドライブとは、SEDでもFIPSでもないドライブです。

Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEでは、Flash Cacheモジュール上のデータは暗号化されません。

外部キー管理を使用する状況

オンボード キー マネージャを使用した方がコストもかからず一般的には便利ですが、次のいずれかに当てはまる場合は外部キー管理を使用する必要があります。

- 組織のポリシーで、FIPS 140-2レベル2（以上）の暗号化モジュールを使用するキー管理ソリューションが求められる場合。
- 暗号化キーを一元管理するマルチクラスタ ソリューションが必要な場合。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

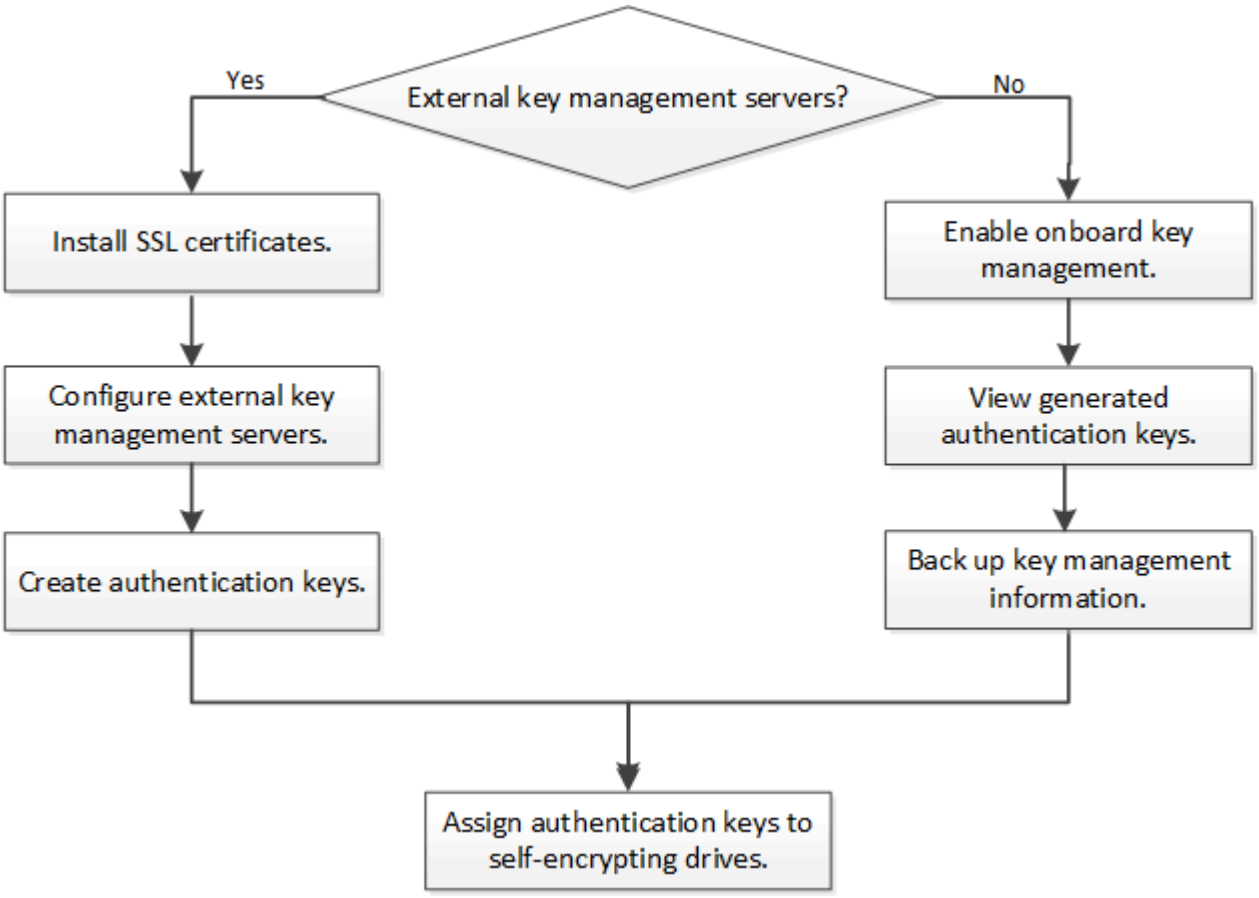
サポートの詳細

次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポート対象のKMIPサーバ、ストレージ システム、ディスク シェルフの最新情報については、Interoperability Matrixを参照してください。

リソースまたは機能	サポートの詳細
異なるタイプのディスクの混在	• FIPSドライブは、同じノードまたはHAペアで他のタイプのドライブと混在させることはできません。準拠したHAペアと準拠していないHAペアを同じクラスタに共存させることは可能です。 • SEDは、同じノードまたはHAペアで非暗号化ドライブと混在させることができます。
ドライブ タイプ	• FIPSドライブには、SASドライブまたはNVMeドライブを使用できます。 • SEDは、NVMeドライブである必要があります。
10Gbネットワーク インターフェイス	ONTAP 9.3以降では、KMIPを使用したキー管理の設定で外部キー管理サーバとの通信に10Gbネットワーク インターフェイスがサポートされます。
キー管理サーバとの通信用のポート	ONTAP 9.3以降では、任意のストレージ コントローラ ポートを使用してキー管理サーバと通信できます。それ以外の場合は、キー管理サーバとの通信にポートe0Mを使用する必要があります。ストレージ コントローラのモデルによっては、ブート プロセス時に一部のネットワーク インターフェイスをキー管理サーバとの通信に使用できない場合があります。
MetroCluster（MCC）	• NVMeドライブではMCCがサポートされます。 • SASドライブではMCCがサポートされません。

ハードウェアベースの暗号化のワークフロー

自己暗号化ドライブに対してクラスタを認証するには、キー管理サービスを設定する必要があります。外部キー管理サーバまたはオンボード キー マネージャを使用できます。



関連情報

- "NetApp Hardware Universe"
- "NetApp Volume Encryption and NetApp Aggregate Encryption"

外部キー管理の設定

ONTAP外部キー管理の設定について学ぶ

1つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードにキーを提供します。

NetApp Volume Encryption（NVE）は、オンボードキーマネージャを使用して実装できます。ONTAP 9.3以降では、外部キー管理（KMIP）とオンボードキーマネージャを使用してNVEを実装できます。ONTAP 9.11.1以降では、クラスタ内に複数の外部キーマネージャを設定できます。クラスター化されたキーサーバーを構成します。を参照してください。

ONTAPクラスタにSSL証明書をインストールする

クラスタとKMIPサーバの間では、相互のIDを検証してSSL接続を確立するためにKMIP SSL証明書を使用します。KMIPサーバとのSSL接続を設定する前に、クラスタのKMIPクライアントSSL証明書、およびKMIPサーバのルートCertificate Authority（CA;認証局

）のSSLパブリック証明書をインストールする必要があります。

タスク概要

HAペア構成では、両方のノードで同じSSL KMIPパブリック証明書とプライベート証明書を使用する必要があります。複数のHAペアを同じKMIPサーバに接続する場合は、HAペアのすべてのノードで同じSSL KMIPパブリック証明書とプライベート証明書を使用する必要があります。

開始する前に

- 証明書を作成するサーバ、KMIPサーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリックSSL KMIPクライアント証明書を入手しておく必要があります。
- クラスタのSSL KMIPクライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIPクライアント証明書は、パスワードで保護しないでください。
- KMIPサーバのルートCertificate Authority（CA;認証局）のSSLパブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

KMIPサーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

手順

1. クラスタにSSL KMIPクライアント証明書をインストールします。

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   SSL KMIPパブリック証明書とプライベート証明書を入力するように求められます。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. KMIPサーバのルート認証局（CA）のSSLパブリック証明書をインストールします。

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

関連情報

- "security certificate install"

ONTAP 9.6以降でハードウェアベースの暗号化の外部キー管理を有効にする

1つ以上のKMIPサーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1つのノードに最大4つのKMIPサーバを接続できます。冗長性とディザスタ リカバリのために少なくとも2つのサーバを使用することを推奨します。

ONTAP 9.11.1以降では、プライマリキーサーバごとに最大3台のセカンダリキーサーバを追加して、クラスタ化されたキーサーバを作成できます。詳細については、クラスタ化された外部キー サーバの設定を参照してください。

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- MetroCluster環境内：
  - 外部キー管理ツールを設定する前に、MetroCluster環境を設定する必要があります。
  - 両方のクラスタに同じ KMIP SSL 証明書をインストールする必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

> ◦ `security key-manager external enable`コマンドは `security key-manager setup`コマンドを置き換えます。 `security key-manager external modify`コマンドを実行すると、外部キー管理の設定を変更できます。"ONTAPコマンド リファレンス"で `security key-manager external enable`の詳細をご覧ください。
> ◦ MetroCluster環境で、管理SVMの外部キー管理を構成する場合は、パートナークラスタで `security key-manager external enable`コマンドを繰り返す必要があります。

次のコマンドは、 `cluster1`の外部キー管理を3つの外部キーサーバで有効にします。最初のキーサーバはホスト名とポートを使用して指定され、2番目はIPアドレスとデフォルトポートを使用して指定され、3番目はIPv6アドレスとポートを使用して指定されます：

```
clusterl::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 設定したすべてのKMIPサーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

> `security key-manager external show-status`コマンドは `security key-manager show -status`
> コマンドを置き換えます。link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAPコマンド リファレンス"^]の `security key-manager external show-status`の詳細を参照してください。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

関連情報

- クラスタ化された外部キー サーバの設定
- "セキュリティキー管理者（外部）を有効化"
- "セキュリティキー・マネージャ外部ステータス表示"

ONTAP 9.5以前でハードウェアベースの暗号化の外部キー管理を有効にする

1つ以上のKMIPサーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1つのノードに最大4つのKMIPサーバを接続できます。冗長性とディザスタ リカバリのために少なくとも2つのサーバを使用することを推奨します。

タスク概要

ONTAPでは、クラスタ内のすべてのノードについてKMIPサーバの接続が設定されます。

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster環境を設定する必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタ ノードのキー管理ツールの接続を設定します。

   ```
   security key-manager setup
   ```

キー管理ツールのセットアップが開始されます。

> MetroCluster環境では、このコマンドを両方のクラスタで実行する必要があります。"ONTAPコマンド リファレンス"の `security key-manager setup`の詳細をご覧ください。

2. 各プロンプトで該当する応答を入力します。
3. KMIPサーバを追加します。

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   > MetroCluster環境では、このコマンドを両方のクラスタで実行する必要があります。

4. 冗長性を確保するためにKMIPサーバをもう1つ追加します。

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   > MetroCluster環境では、このコマンドを両方のクラスタで実行する必要があります。

5. 設定したすべてのKMIPサーバが接続されていることを確認します。

   `security key-manager show -status`

   この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ----------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. 必要に応じて、プレーン テキスト ボリュームを暗号化されたボリュームに変換します。

   `volume encryption conversion start`

   ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

ONTAPでクラスタ化された外部キーサーバを設定する

ONTAP 9.11.1以降では、SVM上でクラスタ化された外部キー管理サーバへの接続を設定できます。クラスタ化されたキーサーバでは、SVM上でプライマリキーサーバとセカンダリキーサーバを指定できます。キーの登録または取得を行う際、ONTAPはまずプライマリキーサーバへのアクセスを試行し、その後、処理が正常に完了するまでセカンダリサーバへのアクセスを順番に試行します。

NetAppストレージ暗号化（NSE）、NetAppボリューム暗号化（NVE）、NetAppアグリゲート暗号化（NAE）のキーには外部キーサーバを使用できます。SVMは最大4台のプライマリ外部KMIPサーバをサポートできます。各プライマリサーバは最大3台のセカンダリキーサーバをサポートできます。

タスク概要

- このプロセスは、KMIPを使用するキーサーバーのみをサポートします。サポートされているキーサーバーのリストについては、"NetApp Interoperability Matrix Tool"をご覧ください。

開始する前に

- "SVMでKMIPキー管理を有効にする必要があります"。
- クラスタのすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- `-secondary-key-servers`パラメータにリストされているサーバーの順序は、外部キー管理（KMIP）サーバーのアクセス順序を反映します。

クラスタ化されたキー サーバの作成

設定手順は、プライマリ キー サーバを設定済みかどうかによって異なります。

SVMへのプライマリ キー サーバとセカンダリ キー サーバの追加

手順

1. クラスタ（admin SVM）に対してキー管理が有効になっていないことを確認します：

   ```
   security key-manager external show -vserver <svm_name>
   ```

   SVMですでに4台のプライマリ キー サーバが有効になっている場合は、新しいプライマリ キー サーバを追加する前に既存のプライマリ キー サーバのいずれかを削除する必要があります。

2. プライマリ キー管理ツールを有効にします。

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - `-key-servers`パラメータでポートを指定しない場合は、デフォルトのポート5696が使用されます。

   > MetroCluster構成内の管理SVMに対して `security key-manager external enable`コマンドを実行する場合は、両方のクラスタでコマンドを実行する必要があります。個別のデータSVMに対してコマンドを実行する場合は、両方のクラスタでコマンドを実行する必要はありません。NetAppでは、両方のクラスタで同じキーサーバを使用することを強くお勧めします。

3. プライマリキーサーバーを変更して、セカンダリキーサーバーを追加します。 `-secondary-key-servers`パラメータには、最大3つのキーサーバーをカンマ区切りで指定できます。

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - `-secondary-key-servers`パラメータにセカンダリキーサーバのポート番号を含めないでください。プライマリキーサーバと同じポート番号が使用されます。

   > MetroCluster構成内の管理SVMに対して `security key-manager external`コマンドを実行する場合は、両方のクラスタでコマンドを実行する必要があります。個別のデータSVMに対してコマンドを実行する場合は、両方のクラスタでコマンドを実行する必要はありません。NetAppでは、両方のクラスタで同じキーサーバを使用することを強くお勧めします。

既存のプライマリ キー サーバへのセカンダリ キー サーバの追加

手順

1. プライマリキーサーバーを変更して、セカンダリキーサーバーを追加します。 `-secondary-key-servers`パラメータには、最大3つのキーサーバーをカンマ区切りで指定できます。

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - `-secondary-key-servers`パラメータにセカンダリ鍵サーバのポート番号を含めないでください。プライマリ鍵サーバと同じポート番号を使用します。

MetroCluster構成内の管理SVMに対して `security key-manager external modify-server`コマンドを実行する場合は、両方のクラスタでコマンドを実行する必要があります。個別のデータSVMに対してコマンドを実行する場合は、両方のクラスタでコマンドを実行する必要はありません。NetAppでは、両方のクラスタで同じキーサーバを使用することを強くお勧めします。

セカンダリキーサーバの詳細については、[mod-secondary]を参照してください。

クラスタ化されたキー サーバの変更

クラスタ化された外部キーサーバは、セカンダリキーサーバの追加と削除、セカンダリキーサーバのアクセス順序の変更、特定のキーサーバの指定（プライマリまたはセカンダリ）の変更によって変更できます。MetroCluster構成内のクラスタ化された外部キーサーバを変更する場合は、NetAppでは両方のクラスタで同じキーサーバを使用することを強くお勧めします。

セカンダリ キー サーバの変更

`security key-manager external modify-server`コマンドの `-secondary-key-servers`パラメータを使用して、セカンダリキーサーバを管理します。 `-secondary-key-servers`パラメータには、カンマ区切りのリストを指定できます。リスト内のセカンダリキーサーバの指定順序によって、セカンダリキーサーバのアクセス順序が決まります。アクセス順序を変更するには、セカンダリキーサーバを異なる順序で入力して `security key-manager external modify-server`コマンドを実行します。セカンダリキーサーバのポート番号は指定しないでください。

MetroCluster構成の管理SVMに対して `security key-manager external modify-server`コマンドを実行する場合は、両方のクラスタでコマンドを実行する必要があります。個々のデータSVMに対してコマンドを実行する場合は、両方のクラスタでコマンドを実行する必要はありません。

セカンダリキーサーバを削除するには、 `-secondary-key-servers`パラメータに保持するキーサーバを含め、削除するキーサーバを省略します。すべてのセカンダリキーサーバを削除するには、引数 `-`を使用します。これは「なし」を意味します。

プライマリ キー サーバとセカンダリ キー サーバの変換

特定のキー サーバーの指定（プライマリまたはセカンダリ）を変更するには、次の手順に従います。

プライマリキーサーバをセカンダリキーサーバに変換

手順

1. SVMからプライマリキーサーバを削除します。

```
security key-manager external remove-servers
```

> MetroCluster構成の管理SVMに対して `security key-manager external remove-servers` コマンドを実行する場合は、両方のクラスタでコマンドを実行する必要があります。個々のデータSVMに対してコマンドを実行する場合は、両方のクラスタでコマンドを実行する必要はありません。

2. 以前のプライマリキーサーバーをセカンダリキーサーバーとして使用してクラスタ化されたキー サーバの作成手順を実行します。

セカンダリキーサーバをプライマリキーサーバに変換する

手順

1. 既存のプライマリキーサーバーからセカンダリキーサーバーを削除します：

```
security key-manager external modify-server -secondary-key-servers
```

- MetroCluster構成の管理SVMに対して `security key-manager external modify-server -secondary-key -servers`コマンドを実行する場合は、両方のクラスタでコマンドを実行する必要があります。個々のデータSVMに対してコマンドを実行する場合は、両方のクラスタでコマンドを実行する必要はありません。
- 既存のキー サーバーを削除しながらセカンダリ キー サーバーをプライマリ キー サーバーに変換する場合、削除と変換が完了する前に新しいキー サーバーを追加しようとすると、キーが重複する可能性があります。

1. 以前のセカンダリキーサーバを新しいクラスタ化されたキーサーバのプライマリキーサーバとして使用して、クラスタ化されたキー サーバの作成手順を実行します。

詳細については、[mod-secondary]を参照してください。

関連情報

- `security key-manager external`の詳細については、"ONTAPコマンド リファレンス"を参照してください

ONTAP 9.6以降での認証キーの作成

`security key-manager key create`コマンドを使用して、ノードの認証キーを作成し、設定されたKMIPサーバに保存できます。

タスク概要

セキュリティの設定によりデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPS準拠の認証キーをデータ アクセスにも

使用できます。

ONTAPでは、クラスタ内のすべてのノードについて認証キーが作成されます。

- このコマンドは、オンボード キー マネージャが有効な場合はサポートされません。ただし、オンボード キー マネージャを有効にすると、2つの認証キーが自動的に作成されます。キーを表示するには、次のコマンドを使用します。

```
security key-manager key query -key-type NSE-AK
```

- 設定済みのキー管理サーバにすでに128個を超える認証キーが格納されている場合は警告が表示されます。
- `security key-manager key delete`コマンドを使用すると、未使用のキーを削除できます。指定したキーが現在ONTAPで使用されている場合、 `security key-manager key delete`コマンドは失敗します。（このコマンドを使用するには、 `admin`以上の権限が必要です。）

> MetroCluster環境では、キーを削除する前に、そのキーがパートナー クラスタで使用されていないことを確認する必要があります。パートナー クラスタで、次のコマンドを使用してキーが使用されていないことを確認してください。
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタ ノードの認証キーを作成します。

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> 設定 `prompt-for-key=true`により、システムはクラスタ管理者に暗号化されたドライブの認証に使用するパスフレーズの入力を求めます。設定しない場合は、システムは32バイトのパスフレーズを自動的に生成します。 `security key-manager key create`コマンドは `security key-manager create-key`コマンドを置き換えます。"ONTAPコマンド リファレンス"の `security key-manager key create`の詳細を確認してください。

次の例では、 `cluster1`の認証キーを作成し、32バイトのパスフレーズを自動的に生成します：

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 認証キーが作成されたことを確認します。

```
security key-manager key query -node node
```

> `security key-manager key query`コマンドは `security key-manager query key`コマンドに置き換わります。

出力に表示されるキーIDは、認証キーへの参照として使用する識別子です。実際の認証キーまたはデータ暗号化キーではありません。

次の例では、`cluster1`の認証キーが作成されたことを確認します：

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

`security key-manager key query`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-query.html["ONTAPコマンド リファレンス"^]をご覧ください。

関連情報

- "storage disk show | more"

ONTAP 9.5以前での認証キーの作成

`security key-manager create-key`コマンドを使用して、ノードの認証キーを作成し、設定されたKMIPサーバに格納できます。

タスク概要

セキュリティの設定によりデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPS準拠の認証キーをデータ アクセスにも使用できます。

ONTAPでは、クラスタ内のすべてのノードについて認証キーが作成されます。

- このコマンドは、オンボード キー管理が有効な場合はサポートされません。
- 設定済みのキー管理サーバにすでに128個を超える認証キーが格納されている場合は警告が表示されます。

  キー管理サーバ ソフトウェアを使用して、使用していないキーを削除してから、コマンドをもう一度実行できます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタ ノードの認証キーを作成します。

   ```
   security key-manager create-key
   ```

   `security key-manager create-key`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-create.html["ONTAPコマンド リファレンス"^]を参照してください。

   出力に表示されるキーIDは、認証キーへの参照として使用する識別子です。実際の認証キーまたはデータ暗号化キーではありません。

   次の例では、`cluster1`の認証キーを作成します：

```
cluster1::> security key-manager create-key
   (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. 認証キーが作成されたことを確認します。

   `security key-manager query`

   `security key-manager query`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-query.html["ONTAPコマンド リファレンス"^]をご覧ください。

   次の例では、 `cluster1`の認証キーが作成されたことを確認します：

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

ONTAP外部キー管理を使用してFIPSドライブまたはSEDにデータ認証キーを割り当てる

`storage encryption disk modify`コマンドを使用して、FIPSドライブまたはSEDにデータ認証キーを割り当てることができます。クラスタノードはこのキーを使用して、ドライブ上の暗号化されたデータをロックまたはロック解除します。

タスク概要

自己暗号化ドライブは、ドライブの認証キーIDがデフォルト以外の値に設定されている場合にのみ、権限のないアクセスから保護されます。SASドライブの場合、標準的なデフォルト値はManufacturer Secure ID（MSID）のキーIDである0x0です。NVMeの標準的なデフォルト値はNULLで、ブランクのキーIDとして表示されます。自己暗号化ドライブにキーIDを割り当てると、認証キーIDがデフォルト以外の値に変更されます。

これはシステムの停止を伴わない手順です。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   ```
   storage encryption disk modify -disk disk_ID -data-key-id key_ID
   ```

`storage encryption disk modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

`security key-manager query -key-type NSE-AK`コマンドを使用してキー ID を表示できます。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

`storage encryption disk show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

関連情報

- "storage disk show | more"
- "storage encryption disk show-status"

オンボード キー管理の設定

オンボード キー管理の有効化（**ONTAP 9.6**以降）

オンボード キー マネージャを使用して、クラスタ ノードをFIPSドライブまたはSEDに

対して認証できます。オンボード キー マネージャは組み込みのツールで、データと同じストレージ システムからノードに認証キーを提供します。オンボード キー マネージャはFIPS-140-2レベル1に準拠しています。

オンボード キー マネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。オンボード キー マネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスク概要

クラスタにノードを追加するたびに、 `security key-manager onboard enable`コマンドを実行する必要があります。MetroCluster構成では、最初にローカルクラスタで `security key-manager onboard enable`を実行し、次にリモートクラスタで `security key-manager onboard sync`を実行する必要があります。その際、各クラスタで同じパスフレーズを使用してください。

`security key-manager onboard enable`および `security key-manager onboard sync`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli//security-key-manager-onboard-enable.html["ONTAPコマンド リファレンス"^]をご覧ください。

デフォルトでは、ノードの再起動時にキーマネージャのパスフレーズを入力する必要はありません。MetroClusterを除き、 `cc-mode-enabled=yes`オプションを使用して、再起動後にユーザーにパスフレーズの入力を求めることができます。

オンボード キー マネージャーが Common Criteria モード(`cc-mode-enabled=yes`で有効になっている場合、システムの動作は次のように変更されます：

- Common Criteriaモードでは、クラスタ パスフレーズの連続入力エラーが監視されます。

  NetApp Storage Encryption（NSE）が有効な場合、ブート時にクラスタの正しいパスフレーズを入力しないと、システムはドライブに対して認証できず、自動的にリブートします。この問題を解決するには、ブート プロンプトで正しいクラスタ パスフレーズを入力する必要があります。ブート後は、クラスタ パスフレーズを求められるコマンドを実行するたびに、クラスタ パスフレーズを24時間以内に5回まで試行することができます。制限に達した場合（例：クラスタ パスフレーズを5回連続で間違えた場合）、24時間のタイムアウト時間が過ぎるのを待つか、またはノードをリブートして制限をリセットする必要があります。

- システム イメージの更新では、通常のNetAppのRSA-2048コード署名証明書とSHA-256のコード署名ダイジェストではなく、NetAppのRSA-3072コード署名証明書とSHA-384のコード署名ダイジェストを使用してイメージの整合性がチェックされます。

  アップグレードコマンドは、様々なデジタル署名をチェックすることで、イメージの内容が改ざんまたは破損していないことを確認します。検証が成功した場合、イメージの更新は次のステップに進みます。検証が失敗した場合、イメージの更新は失敗します。 `cluster image`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

オンボード キー マネージャは揮発性メモリにキーを格納します。揮発性メモリの内容はシステムのリブート時または停止時にクリアされます。通常の動作状態では、揮発性メモリの内容はシステムが停止してから30秒以内にクリアされます。

開始する前に

- NSEで外部キー管理（KMIP）サーバを使用している場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

  "外部キー管理からオンボード キー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボード キー マネージャを設定する前に、MetroCluster環境を設定する必要があります。

手順

1. キー管理ツール セットアップ コマンドを開始します。

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   再起動後にユーザーがキー管理者のパスフレーズを入力する必要があるように `cc-mode-enabled=yes`を設定します。MetroCluster構成では `- cc-mode-enabled`オプションはサポートされていません。 `security key-manager onboard enable`コマンドは `security key-manager setup`コマンドの代わりとなります。

   次の例は、リブートのたびにパスフレーズの入力を求めずに、cluster1でキー管理ツール セットアップ コマンドを開始します。

2. 32文字から256文字までのパスフレーズを入力します。"`cc-mode`"の場合は64文字から256文字までのパスフレーズを入力します。

   指定された「cc-mode」パスフレーズが64文字未満の場合、キー マネージャーのセットアップ操作でパスフレーズ プロンプトが再度表示されるまでに5秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. システムが認証キーを作成したことを確認します：

   ```
   security key-manager key query -node node
   ```

   `security key-manager key query`コマンドは `security key-manager query key`コマンドに置き換わります。

   `security key-manager key query`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-query.html["ONTAPコマンド リファレンス"^]をご覧ください。

終了後の操作

あとで使用できるように、ストレージ システムの外部の安全な場所にパスフレーズをコピーしておきます。

システムは、クラスターの複製データベース（RDB）にキー管理情報を自動的にバックアップします。災害復旧に備えて、この情報を手動でバックアップすることも必要です。

関連情報

- "クラスターイメージコマンド"
- "セキュリティキー・マネージャ外部有効化"
- "セキュリティキー・マネージャーキーのクエリ"
- "セキュリティキー・マネージャーオンボード有効化"
- "外部キー管理からオンボード キー管理への移行"

オンボード キー管理の有効化（ONTAP 9.5以前）

オンボード キー マネージャを使用して、クラスタ ノードをFIPSドライブまたはSEDに対して認証できます。オンボード キー マネージャは組み込みのツールで、データと同じストレージ システムからノードに認証キーを提供します。オンボード キー マネージャはFIPS-140-2レベル1に準拠しています。

オンボードキーマネージャーを使用すると、クラスターが暗号化されたデータにアクセスするために使用するキーを保護できます。暗号化されたボリュームまたは自己暗号化ディスクにアクセスする各クラスターで、オンボードキーマネージャーを有効にしてください。

タスク概要

クラスターにノードを追加するたびに、 `security key-manager setup`コマンドを実行する必要があります。

MetroCluster構成を使用する場合は、次のガイドラインを確認してください。

- ONTAP 9.5 では、ローカルクラスタで `security key-manager setup`を実行し、リモートクラスタで `security key-manager setup -sync-metrocluster-config yes`を実行する必要があります。それぞれ同じパスフレーズを使用します。
- ONTAP 9.5より前では、ローカルクラスタで `security key-manager setup`を実行し、約20秒待ってから、リモートクラスタで `security key-manager setup`を実行し、それぞれで同じパスフレーズを使用する必要があります。

デフォルトでは、ノードの再起動時にキーマネージャのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、 `-enable-cc-mode yes`オプションを使用して、再起動後にユーザーにパスフレーズの入力を要求できます。

NVE の場合、 `-enable-cc-mode yes`を設定すると、 `volume create`コマンドと `volume move start`コマンドで作成したボリュームは自動的に暗号化されます。 `volume create`の場合、 `-encrypt true`を指定する必要はありません。 `volume move start`の場合、 `-encrypt-destination true`を指定する必要はありません。

パスフレーズの試行が失敗した場合は、ノードを再起動する必要があります。

開始する前に

- NSE を外部キー管理（KMIP）サーバーで使用している場合は、外部キー マネージャー データベースを削除します。

  "外部キー管理からオンボード キー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボード キー マネージャーを構成する前に、MetroCluster環境を構成します。

手順

1. キー管理ツールのセットアップを開始します。

   `security key-manager setup -enable-cc-mode yes|no`

   > ONTAP 9.4以降では、 `-enable-cc-mode yes`オプションを使用して、再起動後にユーザーにキーマネージャのパスフレーズの入力を要求できます。NVEの場合、 `-enable-cc-mode yes`を設定すると、 `volume create`コマンドと `volume move start`コマンドで作成したボリュームは自動的に暗号化されます。

   次の例は、リブートのたびにパスフレーズの入力を求めずに、cluster1でキー管理ツールのセットアップを開始します。

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. プロンプトで `yes`を入力して、オンボード キー管理を設定します。
3. パスフレーズプロンプトで、32文字から256文字までのパスフレーズを入力します。または、「`cc-mode`」の場合は64文字から256文字までのパスフレーズを入力します。

   > 指定された「`cc-mode`」パスフレーズが64文字未満の場合、キー マネージャーのセットアップ操作でパスフレーズ プロンプトが再度表示されるまでに5秒の遅延が発生します。

4. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
5. すべてのノードにキーが設定されていることを確認します。

   `security key-manager show-key-store`

   `security key-manager show-key-store`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli-9161/security-key-manager-show-key-store.html["ONTAPコマンドリファレンス"^]をご覧ください。

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

終了後の操作

ONTAPは、キー管理情報をクラスタの複製データベース（RDB）に自動的にバックアップします。

オンボードキーマネージャのパスフレーズを設定したら、その情報をストレージシステム外の安全な場所に手動でバックアップしてください。"オンボード キー管理情報の手動バックアップ"を参照してください。

関連情報

- "オンボード キー管理情報の手動バックアップ"
- "セキュリティキー・マネージャのセットアップ"
- "security key-manager show-key-store"
- "外部キー管理からオンボード キー管理への移行"

ONTAP オンボード キー管理を使用して FIPS ドライブまたは SED にデータ認証キーを割り当てます

`storage encryption disk modify`コマンドを使用して、FIPSドライブまたはSEDにデータ認証キーを割り当てることができます。クラスタノードはこのキーを使用してドライブ上のデータにアクセスします。

タスク概要

自己暗号化ドライブは、ドライブの認証キーIDがデフォルト以外の値に設定されている場合にのみ、権限のないアクセスから保護されます。SASドライブの場合、標準的なデフォルト値はManufacturer Secure ID（MSID）のキーIDである0x0です。NVMeの標準的なデフォルト値はNULLで、ブランクのキーIDとして表示されます。自己暗号化ドライブにキーIDを割り当てると、認証キーIDがデフォルト以外の値に変更されます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   `storage encryption disk modify`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

   `security key-manager key query -key-type NSE-AK`コマンドを使用してキー ID を表示できます。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   `security key-manager key query`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-query.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

   `storage encryption disk show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

関連情報

- "storage disk show | more"
- "storage encryption disk show-status"

ONTAP FIPSドライブにFIPS 140-2認証キーを割り当てる

`storage encryption disk modify`コマンドを `-fips-key-id`オプションとともに使用して、FIPS 140-2認証キーをFIPSドライブに割り当てることができます。クラスタノードは、ドライブへのサービス拒否攻撃の防止など、データアクセス以外のドライブ操作にこのキーを使用します。

タスク概要

セキュリティの設定によっては、データ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合があります。そうでない場合は、FIPS準拠の認証キーをデータ アクセスにも使用できます。

これはシステムの停止を伴わない手順です。

開始する前に

ドライブ ファームウェアはFIPS 140-2準拠をサポートしている必要があります。"NetApp Interoperability Matrix Tool"には、サポートされているドライブ ファームウェア バージョンに関する情報が記載されています。

手順

1. まず、データ認証キーが割り当てられていることを確認する必要があります。これは外部キー マネージャまたはオンボード キー マネージャを使用して行うことができます。キーが割り当てられていることを確認するには、`storage encryption disk show`コマンドを使用してください。
2. SEDにFIPS 140-2認証キーを割り当てます。

   ```
   storage encryption disk modify -disk disk_id -fips-key-id
   fips_authentication_key_id
   ```

   `security key-manager query`コマンドを使用してキー ID を表示できます。

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show -fips`

   `storage encryption disk show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-encryption-disk-show.html["ONTAPコマンド リファレンス"^]を参照してください。

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full <id_value>
2.10.1  full <id_value>
[...]
```

関連情報

- "ストレージ暗号化ディスクの変更"
- "storage disk show | more"
- "storage encryption disk show-status"

ONTAPでKMIPサーバ接続のクラスタ全体のFIPS準拠モードを有効にする

`security config modify`コマンドを-`is-fips-enabled`オプションとともに使用して、転送中のデータに対してクラスタ全体でFIPS準拠モードを有効にすることができます。これにより、クラスタはKMIPサーバへの接続時にFIPSモードでOpenSSLを使用するようになります。

タスク概要

クラスタ全体のFIPS準拠モードを有効にすると、自動的にTLS1.2とFIPS認定暗号スイートのみが使用されます。クラスタ全体のFIPS準拠モードは、デフォルトでは無効になっています。

クラスタ全体のセキュリティの設定を変更した場合は、変更後にクラスタ ノードを手動でリブートする必要があります。

開始する前に

- ストレージ コントローラはFIPS準拠モードで設定する必要があります。
- すべてのKMIPサーバでTLSv1.2がサポートされている必要があります。クラスタ全体のFIPS準拠モードが有効になっている場合、KMIPサーバへの接続を完了するためにTLSv1.2が必要になります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. TLSv1.2がサポートされていることを確認します。

   ```
   security config show -supported-protocols
   ```

   `security config show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-config-show.html["ONTAPコマンド リファレンス"^]を参照してください。

   ```
   cluster1::> security config show
             Cluster                                                 Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                                !aNULL:!EXP:
                                                !eNULL
   ```

3. クラスタ全体のFIPS準拠モードを有効にします。

   ```
   security config modify -is-fips-enabled true -interface SSL
   ```

   `security config modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-config-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

4. クラスタ ノードを手動でリブートします。
5. クラスタ全体のFIPS準拠モードが有効になっていることを確認します。

   ```
   security config show
   ```

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                              !aNULL:!EXP:
                                              !eNULL:!RC4
```

著作権に関する情報

商標に関する情報