NetAppハードウェアベースの暗号化の設定

ONTAP 9

NetApp
December 20, 2024

目次

NetAppハードウェアベースの暗号化の設定

NetAppハードウェアベースの暗号化の設定の概要

NetAppのハードウェアベースの暗号化では、データの書き込み時のフルディスク暗号化（FDE）がサポートされます。ファームウェアに保存されている暗号化キーがないとデータを読み取ることはできません。暗号化キーには、認証されたノードだけがアクセスできます。

NetAppハードウェアベースの暗号化の概要

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に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ともに使用すると、自己暗号化ドライブのデータを「暗号化」できます。

自己暗号化ドライブが有効な場合は、コアダンプも暗号化されます。

> HAペアで暗号化SASドライブまたはNVMeドライブ（SED、NSE、FIPS）を使用している場合は、システムを初期化する前に、HAペア内のすべてのドライブに関連するトピックの手順に従う必要がありますFIPSドライブまたはSEDを非保護モードに戻す（ブートオプション4または9）。これを行わないと、ドライブを転用した場合に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。

- すべてのFASシステムおよびAFFシステムで、自己暗号化機能を備えたFIPS認定のSASドライブまたはNVMeドライブがサポートされます。これらのドライブは _FIPS ドライブと呼ばれ、 Federal Information Processing Standard Publication 140-2 レベル 2 の要件に準拠しています。認定された機能により、ドライブに対するサービス拒否攻撃の防止など、暗号化に加えて保護も可能になります。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。
- ONTAP 9 .6以降では、FIPSテストが完了していない自己暗号化NVMeドライブがAFF A800、A320、およびそれ以降のシステムでサポートされます。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もできます。
- FIPS検証済みドライブはすべて、FIPS検証済みのファームウェア暗号化モジュールを使用します。FIPSドライブ暗号化モジュールは、ドライブ外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は、ドライブのファームウェア暗号化モジュールがキー暗号化キーを取得するために使用されます）。

非暗号化ドライブは、SEDまたはFIPSドライブではないドライブです。

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できるマルチクラスタソリューションが必要です。
- 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。

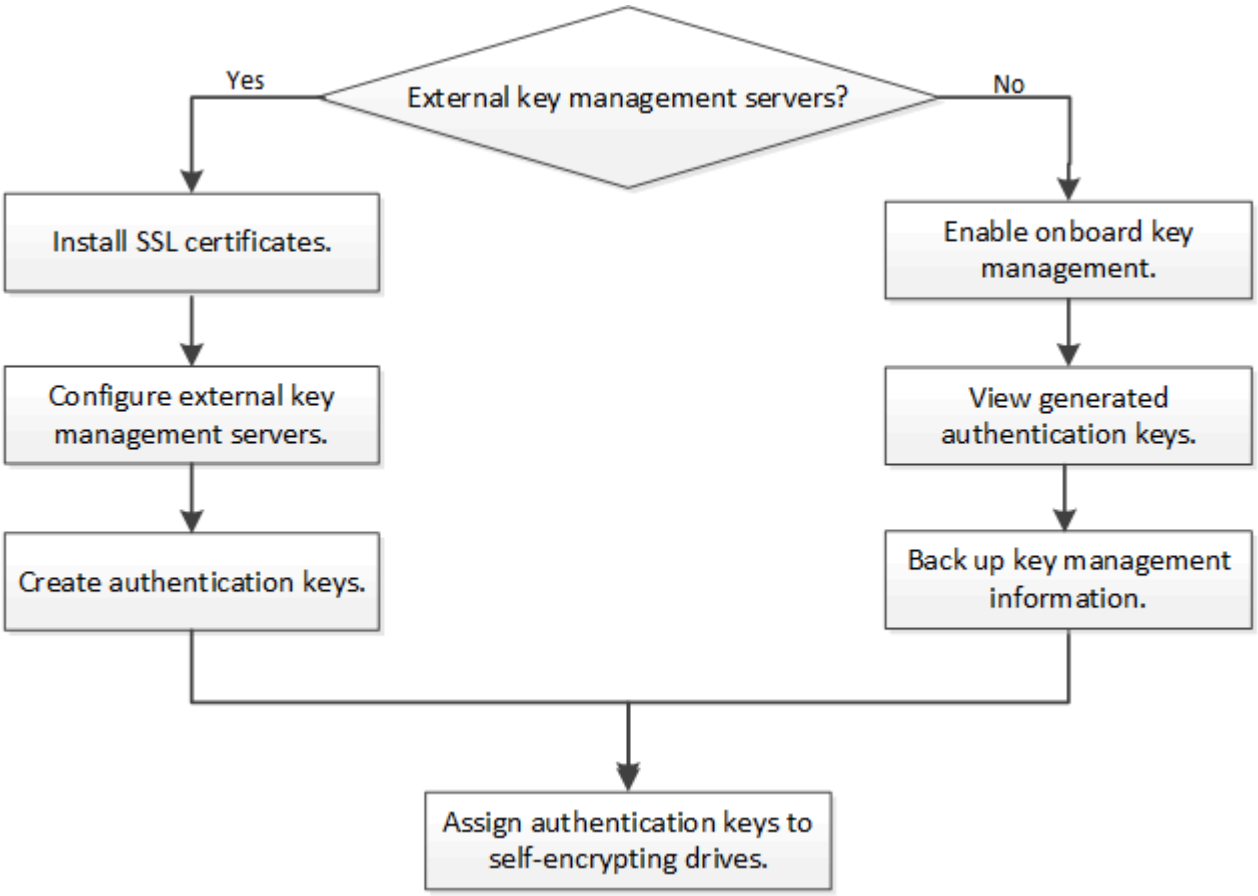
サポートの詳細

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ボリューム暗号化とNetAppアグリゲート暗号化"

外部キー管理の設定

外部キー管理の概要の設定

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ためにクラスタで使用するキーを保護できます。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。

ONTAP 9 .1以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理LIFを割り当てる必要があります。

NetApp Volume Encryption（NVE）は、ONTAP 9 .1以降のオンボードキーマネージャで実装できます。ONTAP 9 .3以降では、NVEを外部キー管理（KMIP）とオンボードキーマネージャで実装できます。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照し クラス

タ化されたキーサーバを設定

ONTAP 9 .2以前でネットワーク情報を収集する

ONTAP 9 .2以前を使用している場合は、外部キー管理を有効にする前に、ネットワーク設定ワークシートに記入してください。

ONTAP 9 .3以降では、必要なすべてのネットワーク情報が自動的に検出されます。

項目	脚注	値
キー管理ネットワークインターフェイス名		
キー管理ネットワークインターフェイスのIPアドレス	ノード管理LIFのIPv4またはIPv6形式のIPアドレス	
キー管理ネットワークインターフェイスのIPv6ネットワークプレフィックス長	IPv6を使用している場合は、IPv6ネットワークプレフィックス長	
キー管理ネットワークインターフェイスのサブネットマスク		
キー管理ネットワークインターフェイスのゲートウェイのIPアドレス		
クラスタネットワークインターフェイスのIPv6アドレス	キー管理ネットワークインターフェイスにIPv6を使用している場合にのみ必要	
各KMIPサーバのポート番号	オプション。ポート番号はすべてのKMIPサーバで同じである必要があります。ポート番号を指定しない場合、デフォルトのポート5696が使用されます。これは、Internet Assigned Numbers Authority（IANA）がKMIPに割り当てたポートです。	
キータグ名	オプション。キータグ名は、ノードに属するすべてのキーを識別するために使用されます。デフォルトのキータグ名はノード名です。	

関連情報

"NetAppテクニカルレポート3954：『NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager』"

"NetAppテクニカルレポート4074：『NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure』"

クラスタへの**SSL**証明書のインストール

クラスタとKMIPサーバは、KMIP SSL証明書を使用して相互のIDを検証し、SSL接続を確立します。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サーバのルート認証局（CA）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。

タスクの内容

HAペアでは、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サーバのルート認証局（CA）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後どちらでも実行できます。

手順

1. クラスタの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の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
   ```

ONTAP 9 .6以降で外部キー管理を有効にする（ハードウェアベース）

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台のサーバが推奨されます。

ONTAP 9 .11.1以降では、プライマリキーサーバごとに最大3つ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、を参照してください クラスタ化された外部キーサーバの設定。

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、コマンドに置き換わるもの `security key-manager setup`です。外部キー管理の設定を変更するには、コマンドを実行し `security key-manager external modify`ます。コマンド構文全体については、マニュアルページを参照してください。
- MetroCluster環境で管理SVMに外部キー管理を設定する場合は、パートナークラスタでこのコマンドを繰り返す必要があります `security key-manager external enable`。

次のコマンドは、3台の外部キーサーバでの外部キー管理を有効にします `cluster1`。1つ目のキーサーバはホスト名とポートを使用して指定し、2つ目のキーサーバはIPアドレスとデフォルトポートを使用して指定し、3つ目のキーサーバはIPv6アドレスとポートを使用して指定します。

```
cluster1::> 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、コマンドに置き換わるもの `security key-manager show -status`です。コマンド構文全体については、マニュアルページ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.
```

ONTAP 9 .5以前で外部キー管理を有効にする（ハードウェアベース）

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台のサーバが推奨されます。

タスクの内容

ONTAPでは、クラスタ内のすべてのノードに対して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環境の場合は、両方のクラスタでこのコマンドを実行する必要があります。

2. 各プロンプトで適切な応答を入力します。

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環境の場合は、両方のクラスタでこのコマンドを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環境の場合は、両方のクラスタでこのコマンドを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`

   コマンド構文全体については、マニュアルページ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でのクラスタ化された外部キーサーバの設定

ONTAP 9.11.1以降では、SVM上の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 サーバを使用すると、1台のSVM上にプライマリ キー サーバとセカンダリ キー サーバを指定できます。キーを登録する際、ONTAPは最初にプライマリ 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各セカ

ンダリ サーバへのアクセスを順次試行して、キーの重複を回避します。

外部キー サーバは、NSE、NVE、NAE、SEDの各キーに使用できます。1台のSVMに最大4台の外部プライマリKMIPサーバを指定できます。各プライマリ サーバには、最大3台のセカンダリ キー サーバを指定できます。

開始する前に

- "SVMでKMIPキー管理が有効になっている必要があります。"です。
- このプロセスでは、KMIPを使用するキーサーバのみがサポートされます。サポートされているキーサーバのリストについては、を参照してください"NetApp Interoperability Matrix Tool"。
- クラスタ内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。
- パラメータ内のserversリストの引数の順序 `-secondary-key-servers`は、外部キー管理（KMIP）サーバのアクセス順序を反映しています。
- 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"

クラスタ化されたキーサーバを作成する

設定手順は、プライマリキーサーバが設定されているかどうかによって異なります。

SVMにプライマリキーサーバとセカンダリキーサーバを追加する

1. クラスタで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ですでに最大4つ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 *server_ip* -client-cert *client_cert_name* -server-ca-certs *server_ca_cert_names*`
3. プライマリキーサーバを変更してセカンダリキーサーバを追加します。 `-secondary-key-servers`パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver *svm_name* -key-servers *primary_key_server* -secondary-key-servers *list_of_key_servers*`

既存のプライマリキーサーバにセカンダリキーサーバを追加する

1. プライマリキーサーバを変更してセカンダリキーサーバを追加します。 `-secondary-key-servers`パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver *svm_name* -key-servers *primary_key_server* -secondary-key-servers *list_of_key_servers*`セカンダリキーサーバの詳細については、を参照してください[mod-secondary]。

クラスタ化されたキーサーバの変更

外部キーサーバクラスタを変更するには、特定のキーサーバのステータス（プライマリまたはセカンダリ）を変更したり、セカンダリキーサーバを追加および削除したり、セカンダリキーサーバのアクセス順序を変更したりします。

プライマリキーサーバとセカンダリキーサーバの変換

プライマリキーサーバをセカンダリキーサーバに変換するには、まずコマンドを使用してそのサーバをSVMから削除する必要があります `security key-manager external remove-servers`。

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には、まず既存のプライマリキーサーバからセカンダリキーサーバを削除する必要があります。を参照して [mod-secondary]既存のキーを削除するときにセカンダリキーサーバをプライマリサーバに変換すると、削除と変換を完了する前に新しいサーバを追加しようとすると、キーが重複することがあります。

セカンダリキーサーバを変更します。

セカンダリキーサーバの管理には、コマンドのパラメータを `security key-manager external modify-server`使用し `-secondary-key-servers`ます。 `-secondary-key-servers`パラメータには、カンマで区切った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した順序によって、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別の順序で入力してコマンドを実行し `security key-manager external modify-server`ます。

セカンダリキーサーバを削除するには、 `-secondary-key-servers`削除するキーサーバを省略して保持するキーサーバを引数に含める必要があります。すべてのセカンダリキーサーバを削除するには、引数（なし）を使用し `-`ます。

リンクhttps://docs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。NetApp .com /us-en/ ONTAP -cli/^][`security key-manager external`コマンドを参照してください。

ONTAP 9 .6以降で認証キーを作成する

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

タスクの内容

セキュリティの設定でデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれに別々 のキーを作成する必要があります。そうでない場合は、FIPSへの準拠にデータアクセスと同じ認証キーを使用できます。

ONTAPでは、クラスタ内のすべてのノードの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になっている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。
- コマンドを使用すると、使用されていないキーを削除できます `security key-manager key delete`。 `security key-manager key delete`指定したキーがONTAPで現在使用されている場合、コマンドは失敗します。(このコマンドを使用するには 'admin より大きい特権が必要です)

MetroCluster環境で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できます。

- `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
```

を設定する `prompt-for-key=true`と、暗号化されたドライブを認証するときに、クラスタ管理者に使用するパスフレーズの入力を求めるプロンプトが表示されます。それ以外の場合は、32バイトのパスフレーズが自動的に生成されます。 `security key-manager key create` コマンドは、コマンドに置き換わるもの `security key-manager create-key`です。コマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーを作成し `cluster1`、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:
000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

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、コマンドに置き換わるもの `security key-manager query key`です。コマンド構文全体については、マニュアルページを参照してください。出力に表示されるキー`ID`は、認証キーの参照に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、の認証キーが作成されたことを確認し `cluster1`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:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

ONTAP 9 .5以前で認証キーを作成する

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

タスクの内容

セキュリティの設定でデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれに別々 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と同じにして使用できます。

ONTAPでは、クラスタ内のすべてのノードの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になっている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未使用のキーを削除してから、コマンドをもう一度実行します。

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
   ```

   完全なコマンド構文については、コマンドのマニュアルページを参照してください。

   出力に表示されるキーIDは、認証キーの参照に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。

   次の例は、の認証キーを作成し `cluster1`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: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   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
   ```

   コマンド構文全体については、マニュアルページを参照してください。

   次の例では、の認証キーが作成されたことを確認し `cluster1`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:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


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

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

FIPSドライブまたはSEDへのデータ認証キーの割り当て（外部キー管理）

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 `storage encryption disk modify`。このキーは、クラスタノードで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するときに使用します。

タスクの内容

自己暗号化ドライブは、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、不正アクセスから保護されます。SASドライブの標準のデフォルト値は、キーIDが0x0のManufacturer Secure ID（MSID；メーカーのセキュアID）です。NVMeドライブの場合、標準のデフォルト値はnullキーで、空のキーIDで表されます。このキーIDを自己暗号化ドライブに割り当てると、認証キーIDがデフォルト以外の値に変更されます。

この手順はシステムの停止を伴いません。

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`

完全なコマンド構文については、コマンドのマニュアルページを参照してください。

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

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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`

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```

オンボードキー管理の設定

ONTAP 9 .6以降でオンボードキー管理を有効にする

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ため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または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。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager onboard enable`ます。`MetroCluster`構成では、同じパスフレーズを使用してまずローカルクラスタでを実行し、次にリモートクラスタでを実行する `security key-manager onboard sync`必要があります `security key-manager onboard enable`。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。MetroClusterの場合を除き、オプションを使用すると、リブート後にユーザにパスフレーズの入力を求めることができます `cc-mode-enabled=yes`。

> オンボードキーマネージャがCCモードで有効になっ(`cc-mode-enabled=yes`ている場合）、システムの動作が次のように変更されます。
>
> - システムは、情報セキュリティ国際評価基準モードで動作しているときに、クラスタパスフレーズの連続した失敗を監視します。
>
> NetAppストレージ暗号化（NSE）が有効になっている場合にブート時に正しいクラスタパスフレーズを入力しないと、システムはドライブを認証できず、自動的にリブートします。これを修正するには、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、クラスタパスフレーズをパラメータとして必要とするコマンドについては、24時間以内に最大5回連続してクラスタパスフレーズを正しく入力できます。制限に達した場合（クラスタパスフレーズを5回連続で正しく入力しなかった場合など）は、24時間のタイムアウト時間が経過するまで待つか、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 RSA-2048コード署名証明書とSHA-256コード署名ダイジェストの代わりに、NetApp RSA-3072コード署名証明書とSHA-384コード署名ダイジェストを使用してイメージの整合性をチェックします。
>
> upgradeコマンドでは、さまざまなデジタル署名をチェックして、イメージの内容が変更または破損していないことを確認します。検証が成功すると、イメージの更新プロセスは次のステップに進みます。それ以外の場合、イメージの更新は失敗します。システムの更新については ' cluster image マニュアル・ページを参照してください

> オンボードキーマネージャは、キーを揮発性メモリに格納します。揮発性メモリの内容は、システムを再起動または停止するとクリアされます。通常の動作状態では、システムが停止すると、揮発性メモリの内容は30秒以内に消去されます。

開始する前に

- NSEで外部キー管理（KMIP）サーバを使用する場合は、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. キー管理ツールのsetupコマンドを開始します。

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

リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるように設定し `cc-mode-enabled=yes`ます。この `- cc-mode-enabled`オプションはMetroCluster構成ではサポートされません。 `security key-manager onboard enable`コマンドは、コマンドに置き換わるもの `security key-manager setup`です。

次の例は、リブートのたびにパスフレーズの入力を要求せずに、cluster1でkey manager setupコマンドを開始します。

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 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. 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、コマンドに置き換わるもの `security key-manager query key`です。コマンド構文全体については、マニュアルページを参照してください。

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

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

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

終了後

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ます。

キー管理情報はすべて、クラスタのReplicated Database（RDB；複製データベース）に自動的にバックアップされます。災害時に備えて、情報を手動でもバックアップしておく必要があります。

ONTAP 9 .5以前でオンボードキー管理を有効にする

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ため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または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。

タスクの内容

このコマンドは、クラスタにノードを追加するたびに実行する必要があり `security key-manager setup`ます。

MetroCluster構成の場合は、次のガイドラインを確認してください。

- ONTAP 9 .5では、同じパスフレーズを使用してローカルクラスタと `security key-manager setup -sync-metrocluster-config yes`リモートクラスタでを実行する必要があります `security key-manager setup`。
- ONTAP 9を実行する前に、同じパスフレーズを使用してローカルクラスタでを実行し、20秒ほど待ってからリモートクラスタでを実行する `security key-manager setup`必要があります `security key-manager setup`。

デフォルトでは、ノードのリブート時にキー管理ツール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、オプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができ `-enable-cc-mode yes`ます。

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

パスフレーズの入力に失敗した場合は、ノードを再起動する必要があります。

開始する前に

- NSEで外部キー管理（KMIP）サーバを使用する場合は、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、オプションを使用して、リブート後にユーザにキー管理ツールのパスフレーズの入力を求めることができます `-enable-cc-mode yes`。NVEでは、を設定する `-enable-cc-mode yes`と、コマンドと `volume move start`コマンドで作成したボリューム `volume create`が自動的に暗号化されます。

   次の例では、リブートのたびにパスフレーズの入力を要求せずに、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. オンボードキー管理を設定するかどうかを確認するプロンプトでと入力し `yes`ます。
3. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

> 指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 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 key show`

   完全なコマンド構文については、マニュアルページを参照してください。

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000100598517 42AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000100 8C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000100598517 42AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000100 8C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

終了後

キー管理情報はすべて、クラスタのReplicated Database（RDB；複製データベース）に自動的にバックアップされます。

オンボードキーマネージャのパスフレーズを設定する場合は、災害時に備えて、ストレージシステムの外部の安全な場所に情報を手動でバックアップする必要があります。を参照して "オンボードキー管理情報の手動でのバックアップ"

FIPSドライブまたはSEDへのデータ認証キーの割り当て（オンボードキー管理）

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 `storage encryption disk modify`。このキーは、クラスタノードでドライブ上のデータにアクセスするときに使用します。

タスクの内容

自己暗号化ドライブは、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、不正アクセスから保護されます。SASドライブの標準のデフォルト値は、キーIDが0x0のManufacturer Secure ID（MSID；メーカーのセキュアID）です。NVMeドライブの場合、標準のデフォルト値はnullキーで、空のキーIDで表されます。このキーIDを自己暗号化ドライブに割り当てると、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`

   完全なコマンド構文については、コマンドのマニュアルページを参照してください。

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4

   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`

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

FIPSドライブへのFIPS 140-2認証キーの割り当て

コマンドでオプションを指定する `-fips-key-id`と、FIPSドライブにFIPS 140-2認証キーを割り当てることができます `storage encryption disk modify`。このキーは、クラスタノードでデータアクセス以外のドライブ処理（ドライブに対するDoS攻撃の防止など）に使用されます。

タスクの内容

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と同じにして使用できます。

この手順はシステムの停止を伴いません。

開始する前に

ドライブファームウェアがFIPS 140-2準拠をサポートしている必要があります。サポートされるドライブファームウェアのバージョンについては、を"NetApp Interoperability Matrix Tool"参照してください。

手順

1. 最初に、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、またはを使用して実行できます外部キー管理ツールオンボードキーマネージャ。コマンドを使用して、キーが割り当てられていることを確認します `storage encryption disk show`。
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`*

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

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

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
   ```

   コマンド構文全体については、マニュアルページ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
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
   2.10.1  full
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
   [...]
   ```

KMIPサーバ接続に対してクラスタ全体のFIPS準拠モードを有効にする

コマンドで`-is-fips-enabled`オプションを使用すると、転送中のデータに対してクラスタ全体の`FIPS`準拠モードを有効にできます `security config modify`。これにより、クラスタからKMIPサーバに接続するときにFIPSモードのOpenSSLが使用されるようになります。

タスクの内容

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検証済みの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設定を変更した場合は、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にはTLSv1.2が必要です。

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
   ```

   コマンド構文全体については、マニュアルページ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`

   コマンド構文全体については、マニュアルページ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