CLIを使用した暗号化の管理

ONTAP 9

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/encryption-at-rest/index.html on December 20, 2024. Always check docs.netapp.com for the latest.

目次

CLIを使用した暗号化の管理

NetApp暗号化の概要

NetAppは、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないように、ソフトウェアベースとハードウェアベースの暗号化テクノロジを提供します。

- NetApp Volume Encryption（NVE）を使用したソフトウェアベースの暗号化で、一度に1つのボリュームのデータ暗号化をサポート
- NetAppストレージ暗号化（NSE）を使用した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。

NetAppボリューム暗号化の設定

NetAppボリューム暗号化の設定の概要

NetApp Volume Encryption（NVE）は、一度に1つのボリュームの保存データを暗号化するためのソフトウェアベースのテクノロジです。暗号化キーにはストレージシステムからしかアクセスできないため、デバイスの転用、返却、置き忘れ、盗難に際してボリュームのデータが読み取られることはありません。

NVEの概要

NVEでは、メタデータとデータ（Snapshotコピーを含む）の両方が暗号化されます。データへのアクセスには、ボリュームごとに1つの一意のXTS-AES-256キーが使用されます。外部キー管理サーバまたはオンボードキーマネージャ（OKM）がノードにキーを提供します。

- 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キーを提供します。

ONTAP 9 .7以降では、Volume Encryption（VE）ライセンスがあり、オンボードまたは外部のキー管理ツールを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。VEライセンスはに含まれてい"ONTAP One"ます。外部キーマネージャまたはオンボードキーマネージャが設定されている場合は、新しいアグリゲートおよび新しいボリュームに対する保存データの暗号化の設定方法が変更されます。新しいアグリゲートでは、NetAppアグリゲート暗号化（NAE）がデフォルトで有効になります。NAEアグリゲートに含まれていない新しいボリュームでは、デフォルトでNetApp Volume Encryption（NVE）が有効になります。マルチテナントキー管理を使用してデータStorage Virtual Machine（SVM）に独自のキー管理機能が設定されている場合、そのSVM用に作成されたボリュームには自動的にNVEが設定されます。

新規または既存のボリュームで暗号化を有効にできます。NVEは、重複排除や圧縮など、さまざまなStorage Efficiency機能をサポートしています。ONTAP 9 .14.1以降では、この機能を既存のSVMルートボリュームでNVEを有効にする使用できます。

SnapLockを使用している場合は、新しい空のSnapLockでのみ暗号化を有効にできます。既存のSnapLockボリュームで暗号化を有効にすることはできません。

NVEは、アグリゲートのタイプ（HDD、SSD、ハイブリッド、アレイLUN）やRAIDタイプを問わず、サポートされているONTAP環境（ONTAP Selectを含む）で使用できます。NVE をハードウェアベースの暗号化と併用すれば、自己暗号化ドライブ上のデータを「暗号化」することもできます。

NVEを有効にすると、コアダンプも暗号化されます。

アグリゲートレベルの暗号化

通常、暗号化されたすべてのボリュームには一意のキーが割り当てられます。このキーは、ボリュームを削除すると一緒に削除されます。

ONTAP 9.6 以降では、 _NetApp Aggregate Encryption （ NAE ） _ を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。暗号化されたボリュームを削除しても、アグリゲートのキーは削除されません。このキーは、アグリゲート全体を削除すると削除されます。

アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。そうしないと、NVEでアグリゲートレベルの重複排除がサポートされません。

ONTAP 9.7以降では、Volume Encryption（VE）ライセンスがあり、オンボード / 外部キー マネージャを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。

NVEボリュームとNAEボリュームは同一アグリゲート内で共存できます。アグリゲートレベルの暗号化で暗号化されたボリュームは、デフォルトでNAEボリュームになります。このデフォルトの設定は、ボリュームを暗号化するときに無効にすることができます。

コマンドを使用して、NVEボリュームをNAEボリュームに（またはその逆に）変換できます `volume move` 。NAEボリュームはNVEボリュームにレプリケートできます。

NAEボリュームではコマンドを使用できません `secure purge`。

外部キー管理サーバを使用する状況

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KMIPサーバを用意する必要があります。

- 暗号化キー管理ソリューションが、Federal Information Processing Standards（FIPS；連邦情報処理標準）140-2またはOASIS KMIP標準に準拠している必要があります。
- 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。

外部キー管理の範囲

外部キー管理の範囲によって、キー管理サーバがクラスタ内のすべてのSVMを保護するか、選択したSVMのみを保護するかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、 *cluster scop* を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。

- ONTAP 9.6 以降では、 *svm scop* を使用して、クラスタ内の指定した SVM に外部キー管理を設定できます。これは、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者のみが、そのテナントのキーにアクセスできます。
- ONTAP 9 .10.1以降では、を使用してNVEキーを保護できるのAzure Key Vault と Google Cloud KMSはデータSVMのみです。これは、9.12.0以降のAWS KMSで利用できるようになりました。

同じクラスタで両方のスコープを使用できます。1つのSVMに対してキー管理サーバが設定されている場合は、それらのサーバのみを使用してキーが保護されます。そうでない場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

検証済みの外部キー管理ツールのリストはにあり"NetApp Interoperability Matrix Tool（IMT）"ます。この一覧は、 IMT の検索機能に「キー管理ツール」という用語を入力すると表示されます。

サポートの詳細

次の表に、NVEのサポートの詳細を示します。

リソースまたは機能	サポートの詳細
プラットフォーム	AES-NIオフロード機能が必要です。ご使用のプラットフォームでNVEとNAEがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

暗号化	ONTAP 9 .7以降では、Volume Encryption（VE）ライセンスを追加し、オンボードまたは外部のキー管理ツールを設定している場合、新しく作成したアグリゲートとボリュームはデフォルトで暗号化されます。暗号化されていないアグリゲートを作成する必要がある場合は、次のコマンドを使用します。
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	プレーンテキストボリュームを作成する必要がある場合は、次のコマンドを使用します。
	
	`volume create -encrypt false`
	
	次の場合、暗号化はデフォルトでは有効になりません。
	
	• VEライセンスがインストールされていません。
	• キー管理ツールが設定されていません。
	• プラットフォームまたはソフトウェアが暗号化をサポートしていません。
	• ハードウェア暗号化が有効になっています。

ONTAP	すべてのONTAP実装。ONTAP 9.5以降では、ONTAP Cloudがサポートされます。
デバイス	HDD、SSD、ハイブリッド、アレイLUN。
RAID	RAID0、RAID4、RAID-DP、RAID-TEC。

ボリューム	データボリュームと既存のSVMルートボリューム。MetroClusterメタデータボリュームのデータは暗号化できません。9.14.1より前のバージョンのONTAPでは、NVEを使用してSVMルートボリュームのデータを暗号化できません。ONTAP 9 .14.1以降では、ONTAPはをサポートしていSVMルートボリュームのNVEます。
アグリゲートレベルの暗号化	ONTAP 9 .6以降では、NVEでアグリゲートレベルの暗号化（NAE）がサポートされます。 • アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。 • アグリゲートレベルで暗号化されたボリュームのキーは変更できません。 • アグリゲートレベルで暗号化されたボリュームでは、セキュア パージがサポートされません。 • NAEでは、データ ボリュームに加えて、SVMルート ボリュームとMetroClusterメタデータ ボリュームの暗号化がサポートされます。ただし、ルート ボリュームの暗号化はサポートされません。
SVMスコープ	ONTAP 9.6以降では、NVEで外部キー管理のみを対象にSVMスコープがサポートされます。オンボード キー マネージャに対してはサポートされません。MetroClusterはONTAP 9.8以降でサポートされます。
Storage Efficiency	重複排除、圧縮、コンパクション、FlexClone。 クローンでは、親からスプリットしたあとも親と同じキーを使用します。スプリットクローンでを実行する必要があり `volume move`ます。この場合、スプリットクローンには別のキーが割り当てられます。
レプリケーション	• ボリュームレプリケーションでは、ソースボリュームとデスティネーションボリュームで異なる暗号化設定を使用できます。暗号化は、ソースに対して設定することも、デスティネーションに対して設定解除することもできます。逆も同様です。ソースで設定された暗号化はデスティネーションにレプリケートされません。暗号化は、ソースとデスティネーションで手動で設定する必要があります。NVEの設定およびを参照してくださいNVEによるボリュームデータの暗号化。 • SVMレプリケーションの場合、デスティネーション ボリュームは自動的に暗号化されます。ただし、ボリューム暗号化をサポートするノードがデスティネーションに含まれていない場合、レプリケーションは成功しますが、デスティネーション ボリュームは暗号化されません。 • MetroCluster構成では、各クラスタが設定されたキー サーバから外部キー管理のキーを取得します。OKM（オンボード キー マネージャ）のキーは、設定レプリケーション サービスによってパートナー サイトにレプリケートされます。
コンプライアンス	ONTAP 9.2以降では、新しいボリュームのみを対象に、SnapLockがComplianceモードとEnterpriseモードの両方でサポートされます。既存のSnapLockボリュームで暗号化を有効にすることはできません。

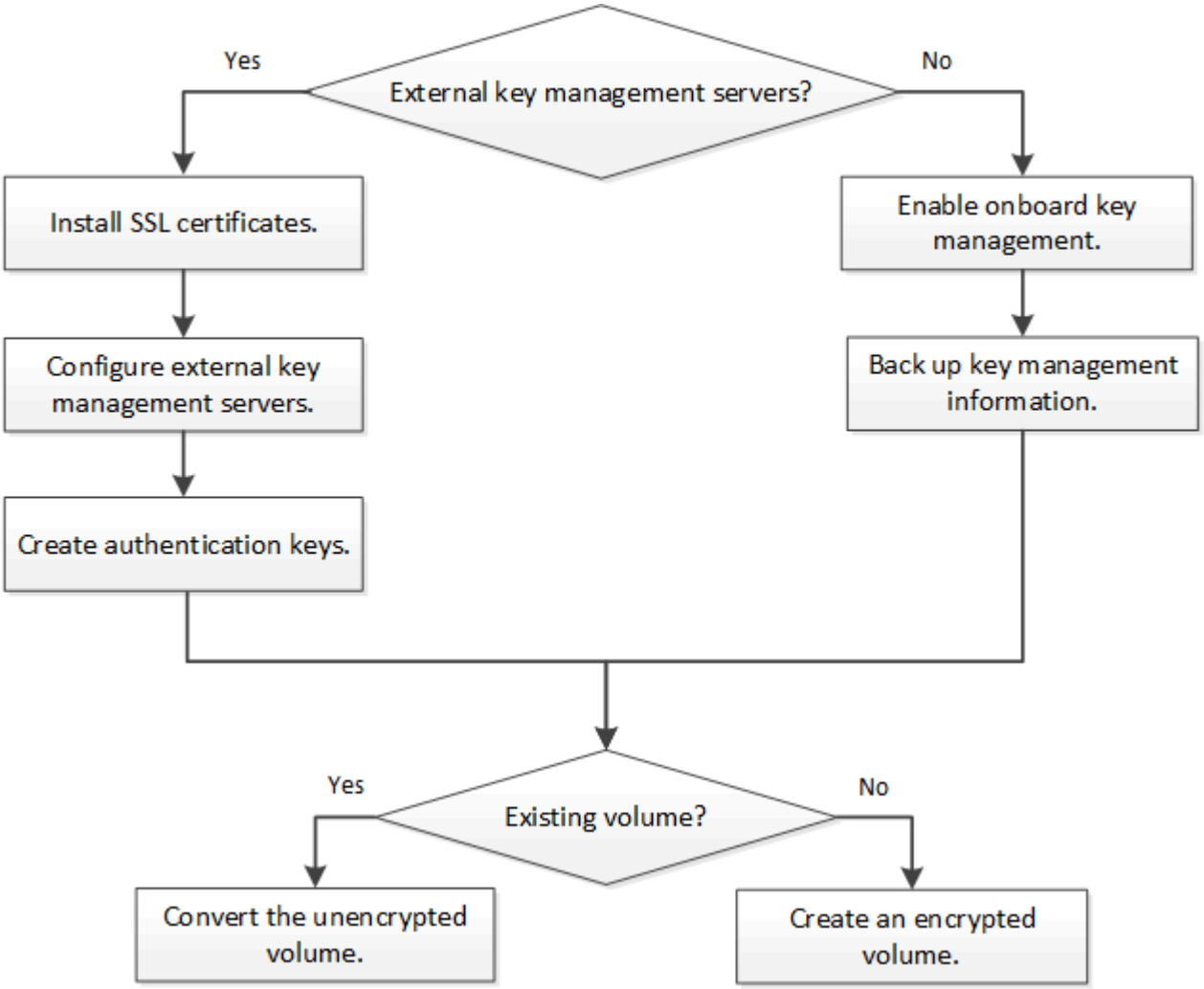
FlexGroup	ONTAP 9.2以降では、FlexGroupがサポートされます。デスティネーション アグリゲートは、ソース アグリゲートと同じタイプ（ボリュームレベルまたはアグリゲートレベル）でなければなりません。ONTAP 9.5以降では、FlexGroupボリュームのキーをインプレースで変更できます。
7-Modeからの移行	7-Mode Transition Tool 3.3以降では、7-Mode Transition Tool CLIを使用して、クラスタ システムのNVE対応デスティネーション ボリュームへのコピーベースの移行を実行できます。

関連情報

"FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"

NetAppボリューム暗号化のワークフロー

ボリューム暗号化を有効にする前に、キー管理サービスを設定する必要があります。新しいボリュームと既存のボリュームのいずれでも暗号化を有効にできます。



"VEライセンスをインストールする必要があります。"NVEでデータを暗号化する前に、キー管理サービスを設定しておく必要があります。ライセンスをインストールする前に、を実行する必要があり"ONTAP のバージョンが NVE をサポートしているかどうかを確認します"ます。

NVEの設定

クラスタのバージョンがNVEをサポートしているかどうかの確認

ライセンスをインストールする前に、クラスタのバージョンがNVEをサポートしているかどうかを確認する必要があります。クラスタのバージョンは、コマンドを使用して確認できます `version`。

タスクの内容

クラスタのバージョンは、クラスタ内のいずれかのノードで実行されているONTAPの最下位のバージョンです。

ステップ

1. クラスタのバージョンがNVEをサポートしているかどうかを確認します。

   ```
   version -v
   ```

   コマンドの出力に「1Ono-DARE」というテキストが表示されている場合、または使用しているプラットフォームがに記載されていない場合は、NVEがサポートされません"サポートの詳細"。

   次のコマンドは、でNVEがサポートされるかどうかを確認し `cluster1`ます。

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   の出力は `1Ono-DARE`、クラスタのバージョンでNVEがサポートされていないことを示しています。

ライセンスをインストールする

VEライセンスでは、クラスタ内のすべてのノードでこの機能を使用できます。このライセンスは、NVEでデータを暗号化する前に必要です。に含まれてい"ONTAP One"ます。

ONTAP Oneより前のバージョンでは、VEライセンスは暗号化バンドルに含まれていました。Encryptionバンドルは提供されなくなりましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は選択できます"ONTAP Oneへのアップグレード"。

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。
- 営業担当者からVEライセンスキーを入手するか、ONTAP Oneをインストールしておく必要があります。

手順

1. "VEライセンスがインストールされていることを確認します。"です。

   VEライセンスパッケージ名はです `VE`。

2. ライセンスがインストールされていない場合は、"System ManagerまたはONTAP CLIを使用してインストール"を参照してください。

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以降でオンボードキーマネージャをサポートしています。ONTAP 9 .3以降では、NVEで外部キー管理（KMIP）とオンボードキーマネージャがサポートされます。NVE .10.1以降では、を使用してONTAP 9キーを保護できますAzure Key VaultサービスまたはGoogle Cloud Key Managerサービス。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

System Managerを使用して外部キー管理ツールを管理します。

ONTAP 9 7以降では、オンボードキーマネージャを使用して認証キーと暗号化キーを格納および管理できます。ONTAP 9 .13.1以降では、外部キー管理ツールを使用してこれらのキーを格納および管理することもできます。

オンボードキーマネージャは、クラスタ内のセキュアなデータベースにキーを格納および管理します。スコープはクラスタです。外部キー管理ツールは、クラスタの外部にキーを格納および管理します。スコープには、クラスタまたはStorage VMを指定できます。1つ以上の外部キー管理ツールを使用できます。次の条件が適用されます。

- オンボードキーマネージャが有効になっている場合、外部キー管理ツールをクラスタレベルで有効にすることはできませんが、Storage VMレベルで有効にすることはできます。
- 外部キー管理ツールがクラスタレベルで有効になっている場合、オンボードキーマネージャを有効にすることはできません。

外部キー管理ツールを使用する場合は、Storage VMおよびクラスタごとに最大4つのプライマリキーサーバを登録できます。各プライマリキーサーバは、最大3台のセカンダリキーサーバでクラスタ化できます。

外部キー管理ツールを設定する

Storage VMに外部キー管理ツールを追加するには、Storage VMのネットワークインターフェイスの設定時にオプションのゲートウェイを追加する必要があります。Storage VMをネットワークルートなしで作成した場合は、外部キー管理ツール用のルートを明示的に作成する必要があります。を参照して "LIFを作成する（ネットワークインターフェイス）"

手順

外部キー管理ツールは、System Managerの別の場所から設定できます。

1. 外部キー管理ツールを設定するには、次のいずれかの開始手順を実行します。

ワークフロー	ナビゲーション	開始ステップ

キーマネージャを設定します	**[クラスタ]**>*[設定]*	[セキュリティ]*セクションまでスクロールします。[暗号化]*で、を選択します。[外部キーマネージャ]*を選択します。
ローカル階層を追加してください	ストレージ>*階層*	[+ローカル階層の追加]*を選択します。[Configure Key Manager]チェックボックスをオンにします。[外部キーマネージャ]*を選択します。
ストレージを準備	ダッシュボード	セクションで、[ストレージの準備]*を選択します。次に、[Configure Key Manager]を選択します。[外部キーマネージャ]*を選択します。
暗号化を設定（キー管理ツールをStorage VMスコープでのみ使用）	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。の[暗号化]*セクションで、を選択します。

2. プライマリキーサーバを追加するには、を選択し Add 、**[IP**アドレス**]**または**[**ホスト名**]***および[ポート]*フィールドに入力します。
3. インストールされている既存の証明書は、**[KMIP Server CA Certificates]***フィールドと[KMIP Client Certificate]*フィールドに表示されます。次のいずれかの操作を実行できます。
   - を選択し て、キー管理ツールにマッピングするインストール済み証明書を選択します。（複数のサービスCA証明書を選択できますが、選択できるクライアント証明書は1つだけです）。
   - まだインストールされていない証明書を追加して外部キー管理ツールにマッピングする場合は、*[新しい証明書の追加]*を選択します。
   - 外部キー管理ツールにマッピングしないインストール済みの証明書を削除するには、証明書名の横にあるを選択し ます。
4. セカンダリキーサーバを追加するには、**[**セカンダリキーサーバ**]***列で[追加]*を選択し、詳細を指定します。
5. [保存]*を選択して設定を完了します。

既存の外部キー管理ツールを編集する

すでに外部キー管理ツールを設定している場合は、その設定を変更できます。

手順

1. 外部キー管理ツールの設定を編集するには、次のいずれかの開始手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	**[クラスタ]**>*[設定]*	セクションまでスクロールします。**[暗号化]***でを選択し、[外部キーマネージャの編集]*を選択します。
Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し、[外部キーマネージャの編集]*を選択します。

2. 既存のキーサーバは*[キーサーバ]*の表に表示されます。次の処理を実行できます。
   - を選択して新しいキーサーバを追加し + Add ます。
   - キーサーバを削除するには、テーブルセルの末尾にあるキーサーバの名前を選択します ⋮ 。そのプライマリキーサーバに関連付けられているセカンダリキーサーバも設定から削除されます。

外部キー管理ツールを削除する

ボリュームが暗号化されていない場合は、外部キー管理ツールを削除できます。

手順

1. 外部キー管理ツールを削除するには、次のいずれかの手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	**[クラスタ]>*[設定]***	セクションまでスクロールします。**[暗号化]***で、を選択し ⋮ 、[外部キーマネージャの削除]*を選択します。
Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し ⋮ 、[外部キーマネージャの削除]*を選択します。

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（NVE）

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。ONTAP 9 .6以降では、独立した外部キー管理ツールを設定して、データSVMが暗号化されたデータにアクセスする際に使用するキーを保護することができます。

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。

タスクの内容

1つのクラスタまたはSVM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。

外部キー管理の範囲によって、キー管理サーバがクラスタ内のすべてのSVMを保護するか、選択したSVMのみを保護するかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、 *cluster scop* を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。
- ONTAP 9.6 以降では、 *svm scop* を使用して、クラスタ内のデータ SVM に外部キー管理を設定できます。これは、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者のみが、そのテナントのキーにアクセスできます。
- マルチテナント環境の場合は、次のコマンドを使用して、 *MT_EK_MGMT* のライセンスをインストールします。

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  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。

同じクラスタで両方のスコープを使用できます。1つのSVMに対してキー管理サーバが設定されている場合は、それらのサーバのみを使用してキーが保護されます。そうでない場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

オンボードキー管理はクラスタスコープで設定し、外部キー管理はSVMスコープで設定できます。コマンド

を使用すると、クラスタスコープのオンボードキー管理からSVMスコープの外部キー管理ツールにキーを移行できます `security key-manager key migrate`。

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、クラスタ管理者またはSVM管理者である必要があります。
- MetroCluster環境で外部キー管理を有効にする場合は、外部キー管理を有効にする前にMetroCluster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。このコマンドをクラスタのログインプロンプトで実行すると、が`*admin_SVM*`デフォルトで現在のクラスタの管理SVMに設定されます。クラスタスコープを設定するには、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。
   - 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 -vserver cluster1 -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. SVMでキー管理ツールを設定します。

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

- このコマンドをSVMのログインプロンプトで実行すると、が `SVM`デフォルトで現在のSVMに設定されます。SVMスコープを設定するには、クラスタ管理者またはSVM管理者である必要があります。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。
- MetroCluster環境でデータSVMの外部キー管理を設定する場合、パートナークラスタでこのコマンドを繰り返す必要はありません `security key-manager external enable`。

次のコマンドは、デフォルトポート5696をリスンする単一のキーサーバでの外部キー管理を有効にします `svm1`。

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. SVMを追加する場合は、最後の手順を繰り返します。

コマンドを使用して追加のSVMを設定することもできます `security key-manager external add-servers`。 `security key-manager external add-servers`コマンドは、コマンドに置き換わるもの `security key-manager add`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。

4. 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
```

`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
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 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 9 .5以前で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`

   ```
   clusterl::> 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`

   ```
   clusterl::> 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。

クラウドプロバイダを使用したキーの管理

ONTAP 9 .10.1以降では、と"Google Cloud Platform のキー管理サービス（ Cloud KMS ）"を使用して、クラウドホストアプリケーションでONTAP暗号化キーを保護できます"Azure キーボールト（ AKV ）"。NVEキーは、ONTAP 9 .12.0以降で保護することもできます"AWS KMS"。

AWS KMS、AKV、およびCloud KMSを使用して保護"NetApp Volume Encryption （ NVE ）キー"できるのは、データSVMの場合のみです。

タスクの内容

クラウドプロバイダを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

クラウドプロバイダを使用してキーを保護する場合は、デフォルトではデータSVM LIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス（Azureの場合はlogin.microsoftonline.com、Cloud KMSの場合はoauth2.googleapis.com）との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

クラウドプロバイダのキー管理サービスを利用する場合は、次の制限事項に注意してください。

- クラウドプロバイダのキー管理は、NetApp Storage Encryption（NSE）およびNetApp Aggregate Encryption（NAE）では使用できません。"外部 KMIP"代わりに使用できます。
- クラウドプロバイダのキー管理はMetroCluster構成では使用できません。
- クラウドプロバイダのキー管理は、データSVMでのみ設定できます。

開始する前に

- 適切なクラウドプロバイダでKMSを設定しておく必要があります。
- ONTAPクラスタのノードでNVEがサポートされている必要があります。
- "Volume Encryption（VE）ライセンスとマルチテナントEncryption Key Management（MTEKM）ライセンスをインストールしておく必要があります。"です。これらのライセンスはに含まれてい"ONTAP One"ます。
- クラスタ管理者またはSVM管理者である必要があります。
- データSVMに暗号化されたボリュームが含まれていないことと、キー管理ツールを使用していないことを確認してください。データSVMに暗号化されたボリュームが含まれている場合は、KMSを設定する前にそれらのボリュームを移行する必要があります。

外部キー管理の有効化

外部キー管理を有効にする方法は、使用するキー管理ツールによって異なります。適切なキー管理ツールと環境のタブを選択します。

AWS

開始する前に

- 暗号化を管理するIAMロールで使用されるAWS KMSキーの付与を作成する必要があります。IAMロールには、次の処理を許可するポリシーが含まれている必要があります。
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`+詳細については、AWSのドキュメントを参照してください"助成金"。

ONTAP SVMでAWS KMVを有効にする

1. 作業を開始する前に、AWS KMSからアクセスキーIDとシークレットキーの両方を取得します。
2. 権限レベルをadvancedに設定します。
   `set -priv advanced`
3. AWS KMSを有効にします。
   `security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. プロンプトが表示されたら、シークレットキーを入力します。
5. AWS KMSが正しく設定されたことを確認します。
   `security key-manager external aws show -vserver svm_name`

Azure

ONTAP SVMでAzure Key Vaultを有効にする

1. 開始する前に、適切な認証クレデンシャル（クライアントシークレットまたは証明書）をAzureアカウントから取得する必要があります。また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用し `cluster show`ます。
2. 特権レベルをadvancedに設定
   `set -priv advanced`
3. SVMでAKVを有効にする
   `security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`プロンプトが表示されたら、クライアント証明書またはAzureアカウントのクライアントシークレットのいずれかを入力します。
4. AKVが正しく有効になっていることを確認します。
   `security key-manager external azure show vserver svm_name`サービスの到達可能性がOKでない場合は、データSVM LIFを介してAKVキー管理サービスへの接続を確立します。

Google Cloud

ONTAP SVMでCloud KMSを有効にする

1. 作業を開始する前に、Google Cloud KMSアカウント キー ファイルの秘密鍵をJSON形式で取得しておきます。これはGCPアカウントから入手できます。また、クラスタ内のすべてのノードが健全であることを確認する必要があります。これを確認するには、コマンドを使用し `cluster show`ます。
2. 特権レベルをadvancedに設定します。
   `set -priv advanced`
3. SVMでCloud KMSを有効にする
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name`

key_ring_name -key-ring-location *key_ring_location* -key-name *key_name*`プロンプトが表示されたら、JSONファイルの内容とサービスアカウントの秘密鍵を入力します。

4. Cloud KMSが正しいパラメータで構成されていることを確認します。
`security key-manager external gcp show vserver *svm_name*`暗号化されたボリュームが作成されていない場合は、のステータス `kms_wrapped_key_status`がになります `"UNKNOWN"。サービスの到達可能性がOKでない場合は、データSVM LIFを介してGCPキー管理サービスへの接続を確立します。

データSVMに対して暗号化されたボリュームがすでに設定されていて、対応するNVEキーが管理SVMのオンボードキーマネージャで管理されている場合は、それらのキーを外部のキー管理サービスに移行する必要があります。これにはCLIを使用して次のコマンドを実行します。
`security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*`データSVMのすべてのNVEキーが正常に移行されるまで、テナントのデータSVM用に暗号化された新しいボリュームを作成できません。

関連情報

- "ネットアップのCloud Volumes ONTAP向け暗号化ソリューションを使用したボリュームの暗号化"

ONTAP 9 .6以降でオンボードキー管理を有効にする（**NVE**）

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 sync`ます。

MetroCluster構成の場合は、同じパスフレーズを使用して最初にローカルクラスタでコマンドを実行してから、リモートクラスタでコマンドを実行する `security key-manager onboard sync`必要があります `security key-manager onboard enable`。ローカルクラスタからコマンドを実行したあとにリモートクラスタで同期する場合、 `security key-manager onboard enable`リモートクラスタからコマンドを再度実行する必要はありません `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。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`。

NVEでは、を設定する `cc-mode-enabled=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`。

保存データの暗号化ONTAPを設定する際に、Commercial Solutions for Classified（CSfC）の要件を満たすためには、NVEとともにNSEを使用し、オンボードキーマネージャをCCモードで有効にする必要があります。CSfCの詳細については、を参照して"CSfC 解決策 Brief （ CSfC の概要"ください。

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。

  ブート時に正しいクラスタパスフレーズを入力しなかった場合、暗号化されたボリュームはマウントされません。これを修正するには、ノードをリブートし、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、のマニュアルページを参照して `cluster image`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

- 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 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。NVEでは、を設定する `cc-mode-enabled=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。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 -key-type NSE-AK`

> ⓘ `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 -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                  Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. 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、オンボードキーマネージャの設定が完了している必要があります。MetroCluster環境では、両方のサイトでオンボードキーマネージャを設定する必要があります。

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。

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"

ONTAP 9 .5以前でオンボードキー管理を有効にする（**NVE**）

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

- 外部キー管理（KMIP）サーバでNSEまたはNVE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
000000000000000002000000000000 1008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000100598517 42AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000 1008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

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、オンボードキーマネージャの設定が完了している必要があります。MetroCluster環境では、両方のサイトでオンボードキーマネージャを設定する必要があります。

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。

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"

新しく追加したノード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、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。

> ONTAP 9 .5以前の場合は、クラスタにノードを追加するたびにコマンドを実行する必要があります `security key-manager setup`。
>
> ONTAP 9 .6以降では、クラスタにノードを追加するたびにコマンドを実行する必要があります `security key-manager sync`。
>
> オンボードキー管理が設定されているクラスタにノードを追加した場合は、このコマンドを実行して不足しているキーを更新します。

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 .6以降では、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`。
- 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。

キー管理ツール間で**ONTAP**データ暗号化キーを移行する

データ暗号化キーは、ONTAPのオンボードキーマネージャまたは外部キー管理ツール（またはその両方）を使用して管理できます。外部キー管理ツールはStorage VMレベルでのみ有効にできます。ONTAPクラスタレベルでは、オンボードキーマネージャまたは外部キーマネージャを有効にできます。

キー管理ツールを有効にする場所	使用できる機能
クラスタレベルのみ	オンボードキーマネージャまたは外部キー管理ツール
SVMレベルのみ	外部キー管理ツールのみ
クラスタレベルとSVMレベルの両方	次のいずれかのキー管理ツールの組み合わせ： • オプション1 クラスタレベル：オンボードキーマネージャ SVMレベル：外部キー管理ツール • オプション2 クラスタレベル：外部キー管理ツール SVMレベル：外部キー管理ツール

ONTAPクラスタレベルでのキー管理ツール間でのキーの移行

ONTAP 9 16.1以降では、ONTAPのコマンドラインインターフェイス（CLI）を使用して、クラスタレベルのキー管理ツール間でキーを移行できます。

オンボードキーマネージャから外部キーマネージャへ

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 非アクティブな外部キー管理ツールの設定を作成します。

```
security key-manager external create-config
```

3. 外部キー管理ツールに切り替えます。

```
security key-manager keystore enable -vserver <svm_name> -type KMIP
```

4. オンボードキーマネージャの設定を削除します。

```
security key-manager keystore delete-config -vserver <svm_name>
-type OKM
```

5. 権限レベルをadminに設定します。

```
set -privilege admin
```

ガイブキーカンリツールカラオンボードキーカンリツールへ

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 非アクティブなオンボードキーマネージャの設定を作成します。

```
security key-manager onboard create-config
```

3. オンボードキーマネージャの設定を有効にします。

```
security key-manager keystore enable -vserver <svm_name> -type OKM
```

4. 外部キー管理ツールの設定を削除します。

```
security key-manager keystore delete-config -vserver <svm_name>
-type KMIP
```

5. 権限レベルをadminに設定します。

```
set -privilege admin
```

ONTAPクラスタレベルとStorage VMレベルのキー管理ツール間でキーを移行

ONTAPのコマンドラインインターフェイス（CLI）を使用して、クラスタレベルのキー管理ツールとStorage VMレベルのキー管理ツールの間でキーを移行できます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. キーを移行します。

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<svm_name>
```

3. 権限レベルをadminに設定します。

```
set -privilege admin
```

NVEによるボリュームデータの暗号化

NVEによるボリュームデータの暗号化の概要

ONTAP 9 .7以降では、VEライセンスがあり、オンボードまたは外部のキー管理を使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。ONTAP 9 .6以前では、新しいボリュームまたは既存のボリュームで暗号化を有効にできます。ボリューム暗号化を有効にする前に、VEライセンスをインストールし、キー管理を有効にしておく必要があります。NVEはFIPS-140-2レベル1に準拠しています。

VEライセンスでアグリゲートレベルの暗号化を有効にする

ONTAP 9 .7以降では"VEライセンス"、およびオンボードまたは外部のキー管理を使用している場合、新しく作成したアグリゲートとボリュームはデフォルトで暗号化されます。ONTAP 9 6以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。

タスクの内容

アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。そうしないと、NVEでアグリゲートレベルの重複排除がサポートされません。

アグリゲートレベルの暗号化が有効になっているアグリゲートは、 _NAE アグリゲートと呼ばれます（ NetApp Aggregate Encryption の場合）。NAEアグリゲート内のすべてのボリュームは、NAEまたはNVE暗号化で暗号化する必要があります。アグリゲートレベルの暗号化では、アグリゲート内に作成するボリュームはデフォルトでNAE暗号化で暗号化されます。デフォルトを上書きしてNVE暗号化を使用することもできます。

NAEアグリゲートではプレーンテキストボリュームはサポートされません。

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. アグリゲートレベルの暗号化を有効または無効にします。

目的	使用するコマンド
ONTAP 9 .7以降でNAEアグリゲートを作成する	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
ONTAP 9 .6を使用してNAEアグリゲートを作成します。	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
NAE以外のアグリゲートをNAEアグリゲートに変換する	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
NAEアグリゲートをNAE以外のアグリゲートに変換する	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

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。

次のコマンドは、でアグリゲートレベルの暗号化を有効にし `aggr1`ます。

- ONTAP 9 .7以降：

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9 .6以前：

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. アグリゲートで暗号化が有効になっていることを確認します。

   `storage aggregate show -fields encrypt-with-aggr-key`

   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。

   次のコマンドは、暗号化が有効になっていることを確認し `aggr1`ます。

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

終了後

コマンドを実行し `volume create`て暗号化されたボリュームを作成します。

ノードの暗号化キーを保存するために KMIP サーバを使用している場合、ボリュームを暗号化すると、ONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

新しいボリュームで暗号化を有効にする

コマンドを使用すると、新しいボリュームで暗号化を有効にできます `volume create`。

タスクの内容

ボリュームは、NetApp Volume Encryption（NVE）およびONTAP 9 .6以降のNetApp Aggregate Encryption（NAE）を使用して暗号化できます。NAEおよびNVEの詳細については、を参照してボリューム暗号化の概要ください。

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

ONTAPの新しいボリュームで暗号化を有効にする手順は、使用しているONTAPのバージョンと特定の構成によって異なります。

- ONTAP 9 4以降では、オンボードキーマネージャのセットアップ時にを有効にした場合、 `cc-mode`コマ

ンドで作成するボリュームは `volume create`、指定したかどうかに関係なく自動的に暗号化され `-encrypt true`ます。

- ONTAP 9 .6以前のリリースでは、コマンドを指定して `volume create`暗号化を有効にする必要があります `-encrypt true`（有効にしていない場合 cc-mode）。
- ONTAP 9でNAEボリュームを作成する場合は、アグリゲートレベルでNAEを有効にする必要があります。6このタスクの詳細については、を参照してくださいVEライセンスでアグリゲートレベルの暗号化を有効にします。
- ONTAP 9 .7以降では"VEライセンス"、およびオンボードまたは外部キー管理を使用している場合、新しく作成したボリュームはデフォルトで暗号化されます。NAEアグリゲート内に作成される新しいボリュームのタイプは、デフォルトではNVEではなくNAEになります。
  - ONTAP 9 .7以降のリリースでは、コマンドに `volume create`を追加してNAEアグリゲートにボリュームを作成すると、 `-encrypt true`そのボリュームではNAEではなくNVE暗号化が使用されます。NAEアグリゲート内のすべてのボリュームは、NVEまたはNAEで暗号化する必要があります。

NAEアグリゲートではプレーンテキストボリュームはサポートされません。

手順

1. 新しいボリュームを作成し、そのボリュームで暗号化を有効にするかどうかを指定します。新しいボリュームがNAEアグリゲートに配置する場合、デフォルトでNAEで暗号化されます。

作成対象	使用するコマンド
NAEボリューム	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name`
NVEボリューム	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true+` NAEがサポートされないONTAP 9 .6以前では、 `-encrypt true`ボリュームをNVEで暗号化するように指定します。NAEアグリゲートにボリュームが作成されるONTAP 9 .7以降では、 `-encrypt true`デフォルトの暗号化タイプであるNAEよりも優先されてNVEボリュームが作成されます。
プレーンテキストボリューム	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false`

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/ volume-create.html[`volume create`^]コマンドを参照してください。

2. ボリュームで暗号化が有効になっていることを確認します。

```
volume show -is-encrypted true
```

コマンド構文全体については、を参照してください "ONTAPコマンド リファレンス"。

結果

ノードの暗号化キーの格納にKMIPサーバを使用している場合は、ボリュームを暗号化するときにONTAPからサーバに暗号化キーが自動的に「プッシュ」されます。

=
:allow-uri-read:

既存のボリュームで暗号化を有効にする

既存のボリュームで暗号化を有効にするには、コマンドまたは `volume encryption conversion start`コマンドを使用し `volume move start`ます。

タスクの内容

- ONTAP 9 3以降では、コマンドを使用して、既存のボリュームの暗号化を「インプレース」で有効にできます `volume encryption conversion start`。ボリュームを別の場所に移動する必要はありません。または、コマンドを使用することもできます `volume move start`。
- ONTAP 9 .2以前では、コマンドのみを使用して、既存のボリュームを移動して暗号化を有効にできます `volume move start`。

volume encryption conversion startコマンドを使用して、既存のボリュームで暗号化を有効にする

ONTAP 9 3以降では、コマンドを使用して、既存のボリュームの暗号化を「インプレース」で有効にできます `volume encryption conversion start`。ボリュームを別の場所に移動する必要はありません。

変換処理を開始したら、完了する必要があります。処理中にパフォーマンスの問題が発生した場合は、コマンドを実行して処理を一時停止し、 `volume encryption conversion resume`コマンドを実行して処理を再開できます `volume encryption conversion pause`。

SnapLockボリュームの変換にはを使用できません `volume encryption conversion start`。

手順

1. 既存のボリュームで暗号化を有効にします。

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

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

   次のコマンドは、既存のボリュームで暗号化を有効にし `vol1`ます。

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   ボリュームの暗号化キーが作成されます。ボリュームのデータが暗号化されます。

2. 変換処理のステータスを確認します。

   `volume encryption conversion show`

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

次のコマンドは、変換処理のステータスを表示します。

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   --------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. 変換処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

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

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

結果

ノードの暗号化キーを保存するために KMIP サーバを使用している場合、ボリュームを暗号化すると、ONTAP によって暗号化キーがサーバに自動的に「プッシュ」されます。

volume move startコマンドを使用して既存のボリュームで暗号化を有効にする

コマンドを使用すると、既存のボリュームを移動して暗号化を有効にできます `volume move start`。ONTAP 9 .2以前ではを使用する必要があります `volume move start`。使用するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

- ONTAP 9 .8以降では、を使用してSnapLockまたはFlexGroupのボリュームで暗号化を有効にでき `volume move start`ます。
- ONTAP 9 .4以降では、オンボードキーマネージャのセットアップ時に「cc-mode」を有効にすると、コマンドで作成するボリュームが自動的に暗号化されます `volume move start`。指定する必要はありません `-encrypt-destination true`。
- ONTAP 9 6以降では、アグリゲートレベルの暗号化を使用して、移動するボリュームの包含アグリゲートにキーを割り当てることができます。一意のキーで暗号化されたボリュームは、_NVEボリューム_と呼ばれます（NetAppボリューム暗号化を使用することを意味します）。アグリゲートレベルのキーで暗号化されたボリュームは、 _NAE ボリューム（ NetApp Aggregate Encryption の場合）と呼ばれます。NAEアグリゲートではプレーンテキストボリュームはサポートされません。
- ONTAP 9 14.1以降では、NVEを使用してSVMルートボリュームを暗号化できます。詳細については、を参照してください SVMルートボリュームでのNetAppボリューム暗号化の設定。

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か、クラスタ管理者から権限を委譲されたSVM管理者である必要があります。

"volume moveコマンドの実行権限の委譲"

手順

1. 既存のボリュームを移動し、そのボリュームで暗号化を有効にするかどうかを指定します。

変換対象	使用するコマンド
プレーンテキストボリュームからNVEボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
NVEボリュームまたはプレーンテキストボリュームからNAEボリューム（デスティネーションでアグリゲートレベルの暗号化が有効になっている場合）	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
NAEボリュームからNVEボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
NAEボリュームからプレーンテキスト ボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
NVEボリュームからプレーンテキストボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前のプレーンテキストボリュームをNVEボリュームに変換し `vol1`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

次のコマンドは、デスティネーションでアグリゲートレベルの暗号化が有効になっている場合に、という名前のNVEボリュームまたはプレーンテキストボリュームをNAEボリュームに変換し `vol1`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

次のコマンドは、という名前のNAEボリュームをNVEボリュームに変換し `vol2`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

次のコマンドは、という名前のNAEボリュームをプレーンテキストボリュームに変換し `vol2`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

次のコマンドは、という名前のNVEボリュームをプレーンテキストボリュームに変換し `vol2`ます。

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. クラスタボリュームの暗号化タイプを表示します。

   `volume show -fields encryption-type none|volume|aggregate`

   この `encryption-type`フィールドは、ONTAP 9 .6以降で使用できます。

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

   次のコマンドは、のボリュームの暗号化タイプを表示します `cluster2`。

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

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

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster2`ます。

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

結果

ノードの暗号化キーの格納にKMIPサーバを使用している場合、ボリュームの暗号化時にONTAPからサーバに暗号化キーが自動的にプッシュされます。

SVMルートボリュームでの**NetApp**ボリューム暗号化の設定

ONTAP 9 14.1以降では、Storage VM（SVM）のルートボリュームでNetApp Volume Encryption（NVE）を有効にすることができます。NVEでは、ルートボリュームが一意のキーで暗号化されるため、SVMのセキュリティが向上します。

タスクの内容

SVMルートボリューム上のNVEは、SVMの作成後にのみ有効にできます。

開始する前に

- NetAppアグリゲート暗号化（NAE）で暗号化されたアグリゲートにSVMルートボリュームを配置しないでください。
- オンボードキーマネージャまたは外部キーマネージャを使用した暗号化を有効にしておく必要があります。
- ONTAP 9.14.1以降が実行されている必要があります。
- NVEで暗号化されたルート ボリュームが含まれるSVMを移行するには、移行の完了後にSVMルート ボリュームをプレーンテキスト ボリュームに変換したうえで、再度SVMルート ボリュームを暗号化する必要があります。
  - SVM移行のデスティネーション アグリゲートでNAEを使用する場合、ルート ボリュームはデフォルトでNAEを継承します。
- SVMがSVMディザスタ リカバリ関係に含まれる場合、次のことに注意してください。
  - ミラーされたSVMの暗号化設定は、デスティネーションにコピーされません。ソースまたはデスティネーションでNVEを有効にする場合は、ミラーされたSVMルート ボリュームで個別にNVEを有効にする必要があります。
  - デスティネーション クラスタ内のすべてのアグリゲートでNAEが使用される場合、SVMルート ボリュームでもNAEが使用されます。

手順

ONTAP CLIまたはSystem Managerを使用して、SVMルートボリュームでNVEを有効にできます。

CLI

NVEは、SVMルートボリュームでインプレースで有効にすることも、アグリゲート間でボリュームを移動することによって有効にすることもできます。

ルートボリュームをインプレースで暗号化

1. ルー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 -vserver svm_name -volume volume
   ```

2. 暗号化が成功したことを確認しますには `volume show -encryption-type volume`、NVEを使用しているすべてのボリュームのリストが表示されます。

SVMルートボリュームの移動による暗号化

1. ボリュームの移動を開始します。

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   の詳細 `volume move`については、を参照してくださいボリュームの移動。

2. コマンドを使用して、処理が成功した `volume move show`ことを確認します `volume move`。には `volume show -encryption-type volume`、NVEを使用しているすべてのボリュームのリストが表示されます。

System Manager

1. ストレージ>ボリュームに移動します。
2. 暗号化するSVMルートボリュームの名前の横にある[Edit]**を選択します ⋮ 。
3. [**Storage and Optimization*]**見出しで、**[** Enable encryption*]を選択します。
4. 保存を選択します。

ノードのルートボリューム暗号化を有効にする

ONTAP 9 8以降では、NetAppボリューム暗号化を使用してノードのルートボリュームを保護できます。

タスクの内容

この手順はノードのルートボリュームに適用されます。SVMルートボリュームには適用されません。SVMルートボリュームは、アグリゲートレベルの暗号化およびで保護できますONTAP 9.14.1以降、NVE。

ルートボリュームの暗号化は、開始後に完了する必要があります。処理を一時停止することはできません。暗号化が完了すると、ルート ボリュームに新しいキーを割り当てられなくなるほか、セキュア パージ処理を実行できなくなります。

開始する前に

- システムでHA構成を使用している必要があります。

- ノードのルートボリュームを作成しておく必要があります。
- オンボードキーマネージャまたはKey Management Interoperability Protocol（KMIP）を使用する外部キー管理サーバがシステムに搭載されている必要があります。

手順

1. ルートボリュームを暗号化します。

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 変換処理のステータスを確認します。

   ```
   volume encryption conversion show
   ```

3. 変換処理が完了したら、ボリュームが暗号化されていることを確認します。

   ```
   volume show -fields
   ```

   次に、暗号化されたボリュームの出力例を示します。

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

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

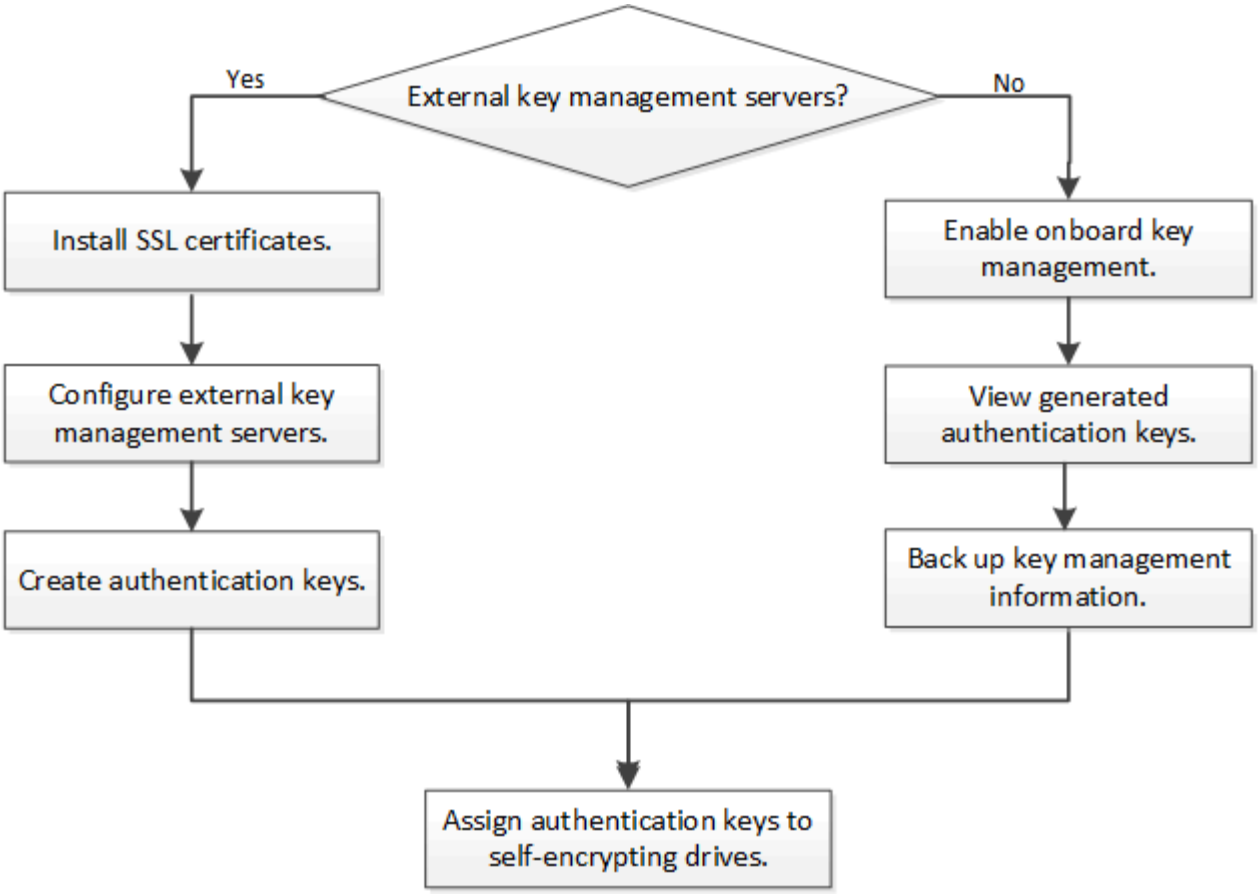
次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポート対象のKMIPサーバ、ストレージ システム、ディスク シェルフの最新情報については、Interoperability Matrixを参照してください。

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
```

NetApp暗号化の管理

ボリュームデータの暗号化解除

コマンドを使用して、ボリュームデータを移動したり暗号化を解除したりできます `volume move start`。

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

手順

1. 既存の暗号化されたボリュームを移動し、ボリュームのデータの暗号化を解除します。

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

   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。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに `aggr3`移動し `vol1`、ボリュームのデータの暗号化を解除します。

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   ボリュームの暗号化キーが削除されます。ボリュームのデータの暗号化が解除されます。

2. ボリュームで暗号化が無効になっていることを確認します。

   `volume show -encryption`

   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。

   次のコマンドは、のボリュームが暗号化されているかどうかを表示します `cluster1`。

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

暗号化されたボリュームを移動する

コマンドを使用すると、暗号化されたボリュームを移動できます `volume move start`。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

デスティネーションノードまたはデスティネーションボリュームでボリューム暗号化がサポートされていない場合、移動は失敗します。

のオプション `volume move start`は `-encrypt-destination`、暗号化されたボリュームに対してはデフォルトでtrueになります。デスティネーションボリュームを暗号化しないように指定すると、ボリューム上のデータの暗号化が誤って解除されることがなくなります。

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。または、クラスタ管理者から権限を委譲

されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

手順

1. 既存の暗号化されたボリュームを移動し、ボリュームのデータを暗号化されたままにします。

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

   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。

   次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに `aggr3`移動し `vol1`、ボリュームのデータを暗号化したままにします。

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   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。

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

   ```
   cluster1::> volume show -is-encrypted true

   Vserver   Volume   Aggregate   State   Type   Size   Available   Used
   -------   ------   ---------   -----   ----   -----   ---------  ----
   vs1       vol1     aggr3      online     RW   200GB     160.0GB   20%
   ```

volume moveコマンドの実行権限を委譲する

コマンドを使用して、既存のボリュームの暗号化、暗号化されたボリュームの移動、またはボリュームの暗号化解除を行うことができます `volume move`。クラスタ管理者は、コマンドを自分で実行することも、コマンドの実行権限をSVM管理者に委譲することもできます `volume move`。

タスクの内容

デフォルトでは、SVM管理者にはロールが割り当て `vsadmin`られます。このロールには、ボリュームを移動する権限は含まれていません。SVM管理者がコマンドを実行できるようにするには、ロールをSVM管理者に `volume move`割り当てる必要があります `vsadmin-volume`。

ステップ

1. コマンドの実行権限を委譲し `volume move`ます。

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role vsadmin-
volume
```

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。

次のコマンドは、SVM管理者にコマンドの実行権限を付与し `volume move`ます。

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

volume encryption rekey startコマンドを使用してボリュームの暗号化キーを変更する

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。ONTAP 9 .3以降では、コマンドを使用して暗号化キーを変更できます `volume encryption rekey start`。

タスクの内容

キー変更処理を開始したら、最後まで完了する必要があります。古いキーに戻ることはできません。処理中にパフォーマンスの問題が発生した場合は、コマンドを実行して処理を一時停止し、 `volume encryption rekey resume`コマンドを実行して処理を再開できます `volume encryption rekey pause`。

キー変更処理が完了するまで、ボリュームには 2 つのキーが存在することになります。新しい書き込みとそれに対応する読み取りでは、新しいキーが使用されます。それ以外の読み取りでは、古いキーが使用されます。

SnapLockボリュームのキー変更にはを使用できません `volume encryption rekey start`。

手順

1. 暗号化キーを変更します。

   ```
   volume encryption rekey start -vserver SVM_name -volume volume_name
   ```

   次のコマンドは、SVMののvs1暗号化キーを変更し `vol1`ます。

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. キー変更処理のステータスを確認します。

   ```
   volume encryption rekey show
   ```

   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。

   次のコマンドは、キー変更処理のステータスを表示します。

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   --------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. キー変更処理が完了したら、ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   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。

   次のコマンドは、上の暗号化されたボリュームを表示し `cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

volume move startコマンドを使用してボリュームの暗号化キーを変更する

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。暗号化キーは、コマンドを使用して変更できます `volume move start`。ONTAP 9 .2以前ではを使用する必要があります `volume move start`。ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

タスクの内容

SnapLockボリュームまたはFlexGroupボリュームのキーの変更にはを使用できません `volume move start`。

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

手順

1. 既存のボリュームを移動し、暗号化キーを変更します。

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   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。

次のコマンドは、という名前の既存のボリュームをデスティネーションアグリゲートに **aggr2**`移動し`**vol1**、暗号化キーを変更します。

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

ボリュームの新しい暗号化キーが作成されます。ボリュームのデータは暗号化されたままです。

2. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

   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。

   次のコマンドは、上の暗号化されたボリュームを表示し`cluster1`ます。

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

NetAppストレージ暗号化の認証キーのローテーション

NetAppストレージ暗号化（NSE）を使用する場合、認証キーをローテーションできます。

タスクの内容

外部キーマネージャ（KMIP）を使用している場合は、NSE環境での認証キーのローテーションがサポートされます。

> オンボードキーマネージャ（OKM）では、NSE環境での認証キーのローテーションはサポートされていません。

手順

1. コマンドを使用し`security key-manager create-key`て、新しい認証キーを生成します。

   認証キーを変更する前に、新しい認証キーを生成する必要があります。

2. コマンドを使用し`storage encryption disk modify -disk * -data-key-id`て、認証キーを変更します。

暗号化されたボリュームを削除する

コマンドを使用すると、暗号化されたボリュームを削除できます `volume delete`。

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。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume move コマンドの実行権限を委譲する"。
- ボリュームはオフラインである必要があります。

ステップ

1. 暗号化されたボリュームを削除します。

   `volume delete -vserver SVM_name -volume volume_name`

   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。

   次のコマンドは、という名前の暗号化されたボリュームを削除し `vol1`ます。

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   削除の確認を求められたら、と入力し `yes`ます。

   ボリュームの暗号化キーは24時間後に削除されます。

   オプションとともに `-force true`使用して、 `volume delete`ボリュームを削除し、対応する暗号化キーをただちに破棄します。このコマンドには高度なPrivilegesが必要です。詳細については、のマニュアルページを参照してください。

終了後

コマンドの実行後、コマンドを使用して、削除したボリュームを保持期間内にリカバリ `volume delete`できます `volume recovery-queue`。

`volume recovery-queue SVM_name -volume volume_name`

"ボリュームリカバリ機能の使用方法"

暗号化されたボリューム上のデータのセキュアパージ

暗号化されたボリューム上のデータのセキュアパージの概要

ONTAP 9 4以降では、セキュアパージを使用して、NVE対応ボリュームのデータを無停止でスクラビングできます。暗号化されたボリュームのデータをスクラビングすることで、「柱」、「ブロックが上書きされたときにデータトレースが残されている」などの物理メディアからデータをリカバリすることができなくなります。また、解約するテナントのデータを安全に削除することもできます。

セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボードキーマネージャではなく、KMIPサーバを使用する必要があります。

- NetApp Aggregate Encryption（NAE）が有効になっているアグリゲートで作成したボリュームでは、セキュアパージはサポートされません。
- セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボードキーマネージャではなく、KMIPサーバを使用する必要があります。

セキュアパージの動作は、ONTAPのバージョンによって異なります。

ONTAP 9.8以降

- セキュアパージはMetroClusterとFlexGroupでサポートされています。
- パージするボリュームがSnapMirror関係のソースである場合は、SnapMirror関係を解除してセキュアパージを実行する必要はありません。
- 再暗号化の方法は、SnapMirrorデータ保護を使用するボリュームとSnapMirrorデータ保護（DP）を使用しないボリューム、またはSnapMirror拡張データ保護を使用するボリュームで異なります。
  - SnapMirrorデータ保護（DP）モードを使用するボリュームでは、デフォルトでボリューム移動再暗号化方式を使用してデータが再暗号化されます。
  - SnapMirrorデータ保護を使用しないボリューム、またはSnapMirror XDP（拡張データ保護）モードを使用するボリュームでは、インプレース再暗号化方式がデフォルトで使用されます。
  - これらのデフォルト値は、コマンドを使用して変更でき `secure purge re-encryption-method [volume-move|in-place-rekey]`ます。
- デフォルトでは、セキュアパージ処理の実行中に、FlexVolボリューム内のすべてのSnapshotコピーが自動的に削除されます。デフォルトでは、FlexGroupおよびSnapMirrorデータ保護を使用するボリューム内のSnapshotは、セキュアパージ処理で自動的に削除されません。これらのデフォルト値は、コマンドを使用して変更でき `secure purge delete-all-snapshots [true|false]`ます。

ONTAP 9 .7以前：

- セキュアパージでは、次の項目はサポートされません。
  - FlexClone
  - SnapVault
  - FabricPool
- パージするボリュームがSnapMirror関係のソースである場合は、ボリュームをパージする前にSnapMirror関係を解除する必要があります。

  ボリューム内に使用中のSnapshotコピーがある場合は、ボリュームをパージする前にSnapshotコピーを解放する必要があります。たとえば、FlexCloneボリュームを親からスプリットする必要がある場合があります。

- セキュアパージ機能を呼び出すと、ボリューム移動がトリガーされ、パージされていない残りのデータが新しいキーで再暗号化されます。

  移動されたボリュームは現在のアグリゲートに残ります。古いキーは自動的に破棄されるため、パージされたデータをストレージメディアからリカバリできません。

ONTAP 9.4 以降では、 NVE 対応ボリューム上で、システムを停止することなく「 crub 」データにセキュアパージを使用できます。

タスクの内容

削除されたファイル内のデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、セキュアパージを実行できません。

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。
- このタスクには高度なPrivilegesが必要です。

手順

1. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
2. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

3. セキュアパージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 削除したファイルのセキュアパージを実行します。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   次のコマンドは、SVM上`vs1`で削除したファイルのセキュアパージを実行し `vol1`ます。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. セキュアパージ処理のステータスを確認します。

   ```
   volume encryption secure-purge show
   ```

ONTAP 9 .8以降では、セキュアパージを使用して、SnapMirror非同期関係にあるNVE対応ボリュームで無停止でデータを「スクラビング」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。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

削除されたファイル内のデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、セキュアパージを実行できません。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
3. 非同期関係のデスティネーションボリュームをセキュアパージする準備をします。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

4. セキュアパージを実行するファイルがSnapshotコピーに含まれている場合は、Snapshotコピーを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. セキュアパージを実行するファイルがベースSnapshotコピーに含まれている場合は、次の手順を実行します。
   a. SnapMirror非同期関係のデスティネーションボリュームにSnapshotコピーを作成します。

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. SnapMirrorを更新してベースのSnapshotコピーを転送します。

```
snapmirror update -source-snapshot snapshot_name -destination-path
destination_path
```

SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

a. 手順（a）と（b）を、ベースSnapshotコピーの数に1を足した数だけ繰り返します。

   たとえば、ベースSnapshotコピーが2つある場合は、手順（a）と（b）を3回繰り返します。

b. ベースのSnapshotコピーが存在することを確認します。+
`snapshot show -vserver SVM_name -volume volume_name`

c. ベースのSnapshotコピーを削除します。+
`snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 削除したファイルのセキュアパージを実行します。

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは、 SVM 「 vs1 」上の「 vol1 」にある削除済みファイルを安全にパージします。

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. セキュアパージ処理のステータスを確認します。

   `volume encryption secure-purge show`

SnapMirror同期関係にある暗号化されたボリュームのデータをスクラビングする

ONTAP 9 8以降では、セキュアパージを使用して、SnapMirror同期関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

タスクの内容

セキュアパージは、削除されたファイル内のデータ量によっては、完了までに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`ます。

> SANホストでセキュアパージを実行するには、パージするファイルを含むLUN全体を削除するか、パージするファイルに属するブロックに対してLUNに穴を開ける必要があります。LUNを削除できない場合や、ホストオペレーティングシステムでLUNのホールパンチングがサポートされていない場合は、セキュアパージを実行できません。

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。
- このタスクには高度なPrivilegesが必要です。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。

3. 非同期関係のデスティネーションボリュームをセキュアパージする準備をします。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   SnapMirror同期関係のもう一方のボリュームに対してこの手順を繰り返します。

4. セキュアパージを実行するファイルがSnapshotコピーに含まれている場合は、Snapshotコピーを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. ベースのSnapshotコピーまたは共通のSnapshotコピーにセキュアパージファイルが含まれている場合は、SnapMirrorを更新して共通のSnapshotコピーを転送します。

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   共通のSnapshotコピーは2つあるため、このコマンドは2回実行する必要があります。

6. セキュアパージファイルがアプリケーションと整合性のあるSnapshotコピーに含まれている場合は、SnapMirror同期関係の両方のボリュームでSnapshotコピーを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   この手順は両方のボリュームで実行します。

7. 削除したファイルのセキュアパージを実行します。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   SnapMirror同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは 'SVM "vs1 `" 上の "vol1" 上の削除されたファイルを安全にパージします

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. セキュアパージ処理のステータスを確認します。

```
volume encryption secure-purge show
```

オンボードキー管理のパスフレーズの変更

セキュリティのベストプラクティスとして、オンボードキー管理のパスフレーズを定期的に変更することが推奨されます。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オンボードキー管理の新しいパスフレーズをコピーしておく必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. オンボードキー管理のパスフレーズを変更します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard update-passphrase`
ONTAP 9.5以前	`security key-manager update-passphrase`

   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ONTAP 9 .6コマンドでは、のオンボードキー管理のパスフレーズを変更でき `cluster1`ます。

   ```
   clusterl::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. オンボードキー管理のパスフレーズを変更するかどうかを確認するプロンプトでと入力し `y`ます。
4. 現在のパスフレーズのプロンプトで現在のパスフレーズを入力します。
5. 新しい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。

6. 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。

終了後

MetroCluster環境では、パートナークラスタでパスフレーズを更新する必要があります。

- ONTAP 9 .5以前では、パートナークラスタで同じパスフレーズを使用してを実行する必要があります `security key-manager update-passphrase`。
- ONTAP 9 .6以降では、パートナークラスタで同じパスフレーズを使用してを実行するように求められます `security key-manager onboard sync`。

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オンボードキー管理のパスフレーズをコピーしておく必要があります。

オンボードキー管理のパスフレーズを変更するときは、キー管理情報を手動でバックアップする必要があります。

"オンボードキー管理情報の手動バックアップ"

オンボードキー管理情報の手動でのバックアップ

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、ストレージシステムの外部の安全な場所にオンボードキー管理の情報をコピーしておく必要があります。

必要なもの

- 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。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

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、キー管理情報を手動でもバックアップしておく必要があります。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスタのキー管理バックアップ情報を表示します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard show-backup`
ONTAP 9.5以前	`security key-manager backup 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。

+次の9.6コマンドは、のキー管理バックアップ情報を表示し `cluster1`ます。

+

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

      ---------------------------BEGIN BACKUP---------------------------
      TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
      QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
      dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
      3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
      IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
      QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
      BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
      AQAAAAMAAAAYAQAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
      AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
      KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
      AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
      LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
      1cNLLwAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAkA
      ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAAJ4/cQsAAAAA
      AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAACQAAAAAAAA
      gAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
      rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      ----------------------------END BACKUP----------------------------
```

1. 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バックアップ情報をコピーします。

オンボードキー管理暗号化キーのリストア

オンボードキー管理の暗号化キーをリストアする手順は、ONTAPのバージョンによって異なります。

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。詳細については、を参照してください。 "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。

> 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。

ONTAP 9.6以降

> ONTAP 9.8以降を実行していてルートボリュームが暗号化されている場合は、の手順を実行します [ontap-9-8]。

1. キーをリストアする必要があることを確認します。+
`security key-manager key query -node node`
2. キーをリストアします。+
`security key-manager onboard sync`

   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ONTAP 9 .6コマンドは、オンボードキー階層のキーを同期します。

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

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

3. パスフレーズのプロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。

ルートボリュームを暗号化した**ONTAP 9.8**以降

ONTAP 9 .8以降を実行しており、ルートボリュームが暗号化されている場合は、ブートメニューでオンボードキー管理のリカバリパスフレーズを設定する必要があります。このプロセスは、ブートメディアを交換する場合にも必要です。

1. ノードをブートメニューでブートし、オプションを選択します `(10) Set onboard key management recovery secrets`。
2. と入力して、 `y`このオプションを使用します。
3. プロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。
4. プロンプトで、バックアップキーのデータを入力します。

   ノードがブートメニューに戻ります。

5. ブートメニューからオプションを選択します `(1) Normal Boot`。

ONTAP 9.5以前

1. キーをリストアする必要があることを確認します。+
`security key-manager key show`

2. ONTAP 9 .8以降を実行していて、ルートボリュームが暗号化されている場合は、次の手順を実行します。

   ONTAP 9 .6または9.7を実行している場合、またはONTAP 9 .8以降を実行していてルートボリュームが暗号化されていない場合は、この手順をスキップします。

3. キーをリストアします。+
   `security key-manager setup -node node`

   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. パスフレーズのプロンプトで、クラスタのオンボードキー管理のパスフレーズを入力します。

外部キー管理の暗号化キーのリストア

外部キー管理の暗号化キーを手動でリストアし、別のノードにプッシュすることができます。この処理は、クラスタのキーの作成時に一時的に停止していたノードを再起動する場合に実行します。

タスクの内容

ONTAP 9 .6以降では、コマンドを使用してキーのリストアが必要かどうかを確認できます `security key-manager key query -node node_name`。

ONTAP 9 .5以前では、コマンドを使用してキーのリストアが必要かどうかを確認できます `security key-manager key show`。

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。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. ONTAP 9 .8以降を実行していて、ルートボリュームが暗号化されている場合は、次の手順を実行します。

   ONTAP 9 .7以前を実行している場合、またはONTAP 9 .8以降を実行していてルートボリュームが暗号化されていない場合は、この手順を省略します。

   a. bootargを設定します。
      ```
      setenv kmip.init.ipaddr <ip-address>
      setenv kmip.init.netmask <netmask>
      setenv kmip.init.gateway <gateway>
      setenv kmip.init.interface e0M++
      boot_ontap
      ```
   b. ノードをブートメニューでブートし、オプションを選択します `(11) Configure node for external key management`。
   c. プロンプトに従って管理証明書を入力します。

      管理証明書の情報をすべて入力すると、システムがブート メニューに戻ります。

d. ブートメニューからオプションを選択します `(1) Normal Boot`。

2. キーをリストアします。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5以前

`node`デフォルトはすべてのノードです。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。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。

次のONTAP 9 .6コマンドは、外部キー管理の認証キーをのすべてのノードにリストアします `cluster1`。

```
clusterl::> security key-manager external restore
```

SSL証明書の交換

すべてのSSL証明書には有効期限があります。認証キーへのアクセスが失われないように、証明書の有効期限が切れる前に証明書を更新する必要があります。

開始する前に

- クラスタの交換用のパブリック証明書と秘密鍵（KMIPクライアント証明書）を入手しておく必要があります。
- KMIPサーバの交換用のパブリック証明書（KMIP server-ca証明書）を入手しておく必要があります。
- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- MetroCluster環境でKMIP SSL証明書を交換する場合は、同じ交換用KMIP SSL証明書を両方のクラスタにインストールする必要があります。

KMIPサーバへの交換用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実行できます。

手順

1. 新しいKMIPサーバCA証明書をインストールします。

```
security certificate install -type server-ca -vserver <>
```

2. 新しいKMIPクライアント証明書をインストールします。

```
security certificate install -type client -vserver <>
```

3. 新しくインストールした証明書を使用するようにキー管理ツールの設定を更新します。

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   MetroCluster環境でONTAP 9 .6以降を実行していて、管理SVMのキー管理ツールの設定を変更する場合は、構成内の両方のクラスタでコマンドを実行する必要があります。

> 新しいクライアント証明書の公開鍵/秘密鍵が以前にインストールした鍵と異なる場合、新しくインストールした証明書を使用するようにキー管理ツールの設定を更新するとエラーが返されます。このエラーを無効にする方法については、ナレッジベースの記事を参照してください"新しいクライアント証明書の公開鍵または秘密鍵が、既存のクライアント証明書と異なります"。

FIPSドライブまたはSEDの交換

FIPSドライブまたはSEDは、通常のディスクと同じ方法で交換できます。交換用ドライブに新しいデータ認証キーを割り当ててください。FIPSドライブの場合は、新しいFIPS 140-2認証キーを割り当てることもできます。

> HAペアでを使用している場合は"SAS ドライブまたは NVMe ドライブの暗号化（ SED 、 NSE 、 FIPS ）"、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対応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。

開始する前に

- ドライブで使用される認証キーのキーIDを確認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。

手順

1. ディスクが障害状態としてマークされていることを確認します。

   ```
   storage disk show -broken
   ```

   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 disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. ディスクシェルフモデルのハードウェアガイドの手順に従って、障害ディスクを取り外し、新しいFIPSドライブまたはSEDに交換します。
3. 交換した新しいディスクの所有権を割り当てます。

   `storage disk assign -disk disk_name -owner node`

   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 disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. 新しいディスク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
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   "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）"

6. 必要に応じて、FIPS 140-2認証キーをFIPSドライブに割り当てます。

   "FIPSドライブへのFIPS 140-2認証キーの割り当て"

FIPSドライブまたはSEDのデータにアクセスできないようにする

FIPSドライブまたはSEDのデータにアクセスできない概要

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブの未使用スペースを新しいデータに使用できるようにしておく場合は、ディスクを完全消去できます。データに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、ディスクを破棄できます。

- ディスク完全消去

  自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID 0x0（SASドライブ）またはnullキー（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去したディスクは、初期化されていないスペアディスクとして再利用できます。

- ディスクの破棄

  FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ディスクが完全にロックされます。これにより、ディスクが永続的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。

完全消去と破棄は、個々の自己暗号化ドライブまたはノードのすべての自己暗号化ドライブに対して実行でき

ます。

FIPSドライブまたは**SED**の完全消去

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、そのドライブを新しいデータに使用する場合は、コマンドを使用してドライブを完全消去できます `storage encryption disk sanitize`。

タスクの内容

自己暗号化ドライブを完全消去すると、ディスク暗号化キーが新しいランダムな値に変更され、電源オンロックの状態がfalseにリセットされ、キーIDがデフォルト値のManufacturer Secure ID 0x0（SASドライブ）またはnullキー（NVMeドライブ）に設定されます。これにより、ディスクのデータにアクセスできない状態になり、データを取得できなくなります。完全消去したディスクは、初期化されていないスペアディスクとして再利用できます。

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. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 完全消去するFIPSドライブまたはSEDのアグリゲートを削除します。

   `storage aggregate delete -aggregate` *`aggregate_name`*

   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 aggregate delete -aggregate aggr1
   ```

3. 完全消去するFIPSドライブまたはSEDのディスクIDを確認します。

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   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
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   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 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. ドライブを完全消去します。

   `storage encryption disk sanitize -disk disk_id`

   このコマンドを使用して完全消去できるのは、ホットスペアディスクまたは破損ディスクのみです。タイプに関係なくすべてのディスクを完全消去するには、オプションを使用し `-force-all-state`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。

   続行する前に、確認フレーズの入力を求めるプロンプトがONTAPに表示されます。画面に表示されたフレーズを正確に入力します。

   ```
   cluster1::> storage encryption disk sanitize -disk 1.10.2

   Warning: This operation will cryptographically sanitize 1 spare or
   broken self-encrypting disk on 1 node.
            To continue, enter sanitize disk: sanitize disk

   Info: Starting sanitize on 1 disk.
         View the status of the operation using the
         storage encryption disk show-status command.
   ```

6. 完全消去したディスクの障害状態を解除します。
   `storage disk unfail -spare true -disk disk_id`
7. ディスクに所有者があるかどうかを確認します
   `storage disk show -disk disk_id`。+ディスクに所有者がない場合は、所有者を割り当てます。
   `storage disk assign -owner node -disk disk_id`
8. 完全消去するディスクを所有するノードのノードシェルに切り替えます。

   `system node run -node node_name`

   コマンドを実行します `disk sanitize release`。

9. ノードシェルを終了します。ディスクの障害状態を再度解除します。

```
storage disk unfail -spare true -disk disk_id
```

10. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
```
storage disk show -disk disk_id
```

FIPSドライブまたはSEDの破棄

FIPSドライブまたはSEDのデータに永久にアクセスできない状態にし、ドライブを再利用する必要もない場合は、コマンドを使用してディスクを破棄できます `storage encryption disk destroy`。

タスクの内容

FIPSドライブまたはSEDを破棄すると、ディスク暗号化キーが不明なランダム値に設定され、ドライブが完全にロックされます。これにより、ディスクが実質的に使用できない状態になり、ディスクのデータに永久にアクセスできなくなります。ただし、ディスクのラベルに印刷されているPhysical Secure ID（PSID；物理的なセキュアID）を使用して、ディスクを工場出荷時の設定にリセットすることができます。詳細については、を参照してください "認証キーが失われた場合にFIPSドライブまたはSEDを使用可能な状態に戻す"。

> 障害ディスク返却不要サービス（NRD Plus）を利用している場合を除き、FIPSドライブまたはSEDは破棄しないでください。ディスクを破棄すると保証が無効になります。

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. 保持する必要があるデータを別のディスク上のアグリゲートに移行します。
2. 破棄する FIPS ドライブまたは SED のアグリゲートを削除します。

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   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 aggregate delete -aggregate aggr1
   ```

3. 破棄する FIPS ドライブまたは SED のディスク ID 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
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. ディスクを破棄します。

   `storage encryption disk destroy -disk disk_id`

   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。

   続行する前に確認のフレーズを入力するように求められます。画面に表示されたフレーズを正確に入力します。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

FIPSドライブまたは**SED**の緊急時のシュレッドデータ

セキュリティに関する緊急事態が発生した場合は、ストレージシステムまたはKMIPサーバへの給電が遮断されていても、FIPSドライブまたはSEDへのアクセスを即座に禁止できます。

開始する前に

- 使用可能な電力が供給されていないKMIPサーバを使用している場合は、破棄しやすい認証アイテム（スマートカードやUSBドライブなど）を使用してKMIPサーバを設定する必要があります。

- 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。

ステップ

1. FIPSドライブまたはSEDのデータの緊急時のシュレッディングを実行します。

状況	そしたら…。

ストレージシステムに給電されており、ストレージシステムを正常にオフラインにする時間がある	a. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。
	b. すべてのアグリゲートをオフラインにしてから削除します。
	c. 権限レベルをadvancedに設定します。+
	`set -privilege advanced`
	d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。+
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. ストレージシステムを停止します。
	f. メンテナンスモードでブートします。
	g. ディスクを完全消去するか破棄します。
	◦ ディスクのデータにアクセスできない状態にしてディスクを再利用する場合は、ディスクを完全消去します。+
	`disk encrypt sanitize -all`
	◦ ディスクのデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄します。+
	`disk encrypt destroy disk_id1 disk_id2 …`
		ストレージシステムに給電されており、データをただちにシュレッディングする必要がある

a. * ディスク上のデータにアクセスできない状態にし、ディスクを再利用する場合は、ディスクを完全消去します。 *
b. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。
c. 権限レベルをadvancedに設定します。
`set -privilege advanced`
d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. ディスクを完全消去します。
`storage encryption disk sanitize -disk * -force-all-states true`
	a. * ディスク上のデータにアクセスできない状態にし、ディスクを保存する必要もない場合は、ディスクを破棄してください： *
	b. ストレージシステムがHAペアとして構成されている場合は、テイクオーバーを無効にします。
	c. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	d. ディスクを破棄します。
	`storage encryption disk destroy -disk * -force-all-states true`
		ストレージシステムがパニック状態になり、システムは永続的に無効な状態になり、すべてのデータが消去されます。システムを再度使用するには、再設定する必要があります。

KMIPサーバに給電されているが、ストレージシステムには給電されていない	a. KMIPサーバにログインします。 b. アクセスを禁止するデータを含むFIPSドライブまたはSEDに関連付けられているすべてのキーを破棄します。これにより、ストレージシステムからディスク暗号化キーにアクセスできなくなります。	KMIPサーバまたはストレージシステムに給電されていない

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。

認証キーが失われた場合に**ONTAP**を使用して**FIPS**ドライブまたは**SED**を使用可能な状態に戻す

FIPSドライブまたはSEDの認証キーが永久に失われ、KMIPサーバから取得できない場合、FIPSドライブまたはSEDは破損しているとみなされます。ディスク上のデータにアクセスしたりリカバリしたりすることはできませんが、SEDの未使用スペースをデータに再び使用できるようにすることができます。

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。

タスクの内容

このプロセスは、FIPSドライブまたはSEDの認証キーが永久に失われてリカバリできないことが確実である場合にのみ使用してください。

ディスクがパーティショニングされている場合は、このプロセスを開始する前にパーティショニングを解除する必要があります。

ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用でき、NetAppサポートから指示があった場合にのみ実行してください。続行する前に、ネットアップサポートにお問い合わせください。ナレッジベースの記事も参照できます"ONTAP でスペアドライブのパーティショニングを解除する方法"。

手順

1. FIPSドライブまたはSEDを使用可能な状態に戻します。

SED の状況	実行する手順

FIPS準拠モードではない、またはFIPS準拠モードでFIPSキーを使用できる	a. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	b. FIPSキーをデフォルトのメーカーセキュアIDである0x0にリセットします。
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 処理が成功したことを確認します。
	`storage encryption disk show-status`処理に失敗した場合は、このトピックのPSIDプロセスを使用してください。
	d. 破損ディスクを完全消去します。次の手順に進む前に、コマンドを使用して処理が成功したことを確認します `storage encryption disk show-status`。
	`storage encryption disk sanitize -disk disk_id`
	e. 完全消去したディスクの障害状態を解除します。
	`storage disk unfail -spare true -disk disk_id`
	f. ディスクに所有者があるかどうかを確認します
	`storage disk show -disk disk_id`。+ディスクに所有者がない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk disk_id`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node node_name`
	コマンドを実行します `disk sanitize release`。
	g. ノードシェルを終了します。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk disk_id`
	h. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk disk_id`

FIPS準拠モードでFIPSキーを使用できず、SEDのPSIDがラベルに印刷されている	a. ディスクラベルからディスクのPSIDを確認します。
	b. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	c. ディスクを工場出荷時の設定にリセットします。次の手順に進む前に、コマンドを使用して処理が成功したことを確認し `storage encryption disk show-status`ます。
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`
	d. ONTAP 9.8P5以前を実行している場合は、次の手順に進みます。ONTAP 9 .8P6以降を実行している場合は、完全消去したディスクの障害状態を解除します。
	`storage disk unfail -disk disk_id`
	e. ディスクに所有者があるかどうかを確認します
	`storage disk show -disk disk_id`。+ディスクに所有者がない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk disk_id`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node node_name`
	コマンドを実行します `disk sanitize release`。
	f. ノードシェルを終了します。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk disk_id`
	g. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk disk_id`

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

FIPSドライブまたはSEDを非保護モードに戻します。

FIPSドライブまたはSEDは、ノードの認証キーIDがデフォルト以外の値に設定されている場合にのみ不正アクセスから保護されます。FIPSドライブまたはSEDを非保護モードに戻すには、コマンドを使用して `storage encryption disk modify`キーIDをデフォルトに設定します。

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でこのプロセスを実行する必要があります（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。

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. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. FIPSドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   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 2.10.11 -fips-key-id
   0x0

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

   コマンドを使用して、処理が成功したことを確認します。

   ```
   storage encryption disk show-status
   ```

   「Disks Begin」と「Disks Done」の数値が同じになるまで、show-statusコマンドを繰り返します。

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start               Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp           Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------  ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. ノードのデータ認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   storage encryption disk modify -disk disk_id -data-key-id 0x0
   ```

   SASドライブとNVMeドライブのどちらを非保護モードに戻すかに関係なく、の値は `-data-key-id`0x0に設定する必要があります。

   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 2.10.11 -data-key-id
0x0

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

コマンドを使用して、処理が成功したことを確認します。

```
storage encryption disk show-status
```

番号が同じになるまで、show-statusコマンドを繰り返します。処理が完了するのは、「ディスクの開始」と「ディスクの終了」の番号が同じ場合です。

メンテナンスモオト

ONTAP 9 .7以降では、保守モードからFIPSドライブのキーを変更できます。保守モードは、前述のONTAP CLIの手順を使用できない場合にのみ使用してください。

手順

1. ノードのFIPS認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   disk encrypt rekey_fips 0x0 disklist
   ```

2. ノードのデータ認証キーIDをデフォルトのMSIDである0x0に戻します。

   ```
   disk encrypt rekey 0x0 disklist
   ```

3. FIPS認証キーのキーが正常に変更されたことを確認します。

   ```
   disk encrypt show_fips
   ```

4. データ認証キーのキーが変更されたことを確認します。

   ```
   disk encrypt show
   ```

   出力には、デフォルトのMSID 0x0キーIDまたはキーサーバが保持する64文字の値が表示される可能性があります。 `Locked?`フィールドはデータロックを参照します。

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

外部キー管理ツールの接続を削除する

KMIPサーバが不要になったときはノードから切断できます。たとえば、ボリューム暗号

化に移行するときにKMIPサーバを切断できます。

タスクの内容

HAペアの一方のノードからKMIPサーバを切断すると、すべてのクラスタノードから自動的にサーバが切断されます。

KMIPサーバを切断したあとも外部キー管理を引き続き使用する場合は、別のKMIPサーバで認証キーを提供できることを確認してください。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

ステップ

1. 現在のノードからKMIPサーバを切断します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5以前

MetroCluster環境の場合は、管理SVMの両方のクラスタでこれらのコマンドを繰り返す必要があります。

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。

次のONTAP 9 .6コマンドは、2つの外部キー管理サーバへの接続を無効にします。1つ目はデフォルトポート5696をリスンするという名前のサーバ、 `ks1`もう1つはポート24482をリスンするIPアドレス10.0.0.20のサーバ `cluster1`です。

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

外部キー管理サーバのプロパティを変更します。

ONTAP 9 .6以降では、コマンドを使用して外部キー管理サーバのI/Oタイムアウトとユーザ名を変更でき `security key-manager external modify-server`ます。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。
- このタスクには高度なPrivilegesが必要です。
- MetroCluster環境の場合は、管理SVMの両方のクラスタで上記の手順を繰り返す必要があります。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. クラスタの外部キー管理サーバのプロパティを変更します。

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。このコマンドをクラスタのログインプロンプトで実行すると、が`*admin_SVM*`デフォルトで現在のクラスタの管理SVMに設定されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者である必要があります。

次のコマンドは、デフォルトポート5696をリスンしている外部キー管理サーバのタイムアウト値を45秒に変更します `cluster1`。

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. SVMの外部キー管理サーバのプロパティを変更します（NVEのみ）。

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。このコマンドをSVMのログインプロンプトで実行すると、が`*SVM*`デフォルトで現在のSVMに設定されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者またはSVM管理者である必要があります。

次のコマンドは、デフォルトポート5696をリスンする外部キー管理サーバのユーザ名とパスワードを変更し`svm1`ます。

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. SVMを追加する場合は、最後の手順を繰り返します。

オンボードキー管理から外部キー管理への移行

オンボードキー管理から外部キー管理に切り替える場合は、外部キー管理を有効にする前にオンボードキー管理の設定を削除する必要があります。

開始する前に

- ハードウェアベースの暗号化の場合は、すべてのFIPSドライブまたはSEDのデータキーをデフォルト値にリセットする必要があります。

"FIPSドライブまたはSEDを非保護モードに戻す"

- ソフトウェアベースの暗号化では、すべてのボリュームの暗号化を解除する必要があります。

  "ボリューム データの暗号化の解除"

- 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。

ステップ

1. クラスタのオンボードキー管理の設定を削除します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5以前	`security key-manager delete-key-database`

コマンド構文全体については、を参照してください "ONTAPコマンド リファレンス"。

外部キー管理からオンボードキー管理への移行

外部キー管理からオンボードキー管理に切り替える場合は、オンボードキー管理を有効にする前に外部キー管理の設定を削除する必要があります。

開始する前に

- ハードウェアベースの暗号化の場合は、すべてのFIPSドライブまたはSEDのデータキーをデフォルト値にリセットする必要があります。

  "FIPSドライブまたはSEDを非保護モードに戻す"

- すべての外部キー管理ツールの接続を削除しておく必要があります。

  "外部キー管理ツールの接続の削除"

- 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

キー管理の移行手順は、使用しているONTAPのバージョンによって異なります。

ONTAP 9.6以降

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを使用します。

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   MetroCluster環境の場合は、管理SVMに対して両方のクラスタでこのコマンドを繰り返す必要があります。

ONTAP 9.5以前

次のコマンドを使用します。

```
security key-manager delete-kmip-config
```

ブートプロセス中にキー管理サーバにアクセスできない場合の動作

ブートプロセス時に NSE 用に構成されたストレージシステムが指定されたどのキー管理サーバにもアクセスできない場合、 ONTAP ではストレージシステムの望ましくない動作を回避するために、特定の予防措置を取ります。

ストレージシステムが NSE 用に設定されている場合、 SED のキーが変更されてロックされ、 SED の電源がオンになっているときは、ストレージシステムは、キー管理サーバから必要な認証キーを取得して SED に対して自身を認証し、データにアクセスできるようにする必要があります。

ストレージシステムは、指定されたキー管理サーバへのアクセスを最大 3 時間試行します。その時間が経過してもストレージシステムがどのキー管理サーバにもアクセスできない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムは、指定されたいずれかのキー管理サーバに正常にアクセスできた場合、SSL接続の確立を最大15分間試行します。ストレージシステムが指定されたどのキー管理サーバとも SSL 接続を確立できない場合は、ブートプロセスが停止して、ストレージシステムも停止します。

ストレージシステムがキー管理サーバへのアクセスと接続を試行している間、失敗したアクセス試行に関する詳細情報がCLIに表示されます。アクセスの試行は、 Ctrl+C キーを押すことによっていつでも中断できます

セキュリティ対策として、SEDでは許可される不正アクセスの試行回数が制限され、試行回数が制限されたあとは既存データへのアクセスが無効になります。ストレージシステムが指定されたどのキー管理サーバにもアクセスできず、適切な認証キーを取得できない場合、デフォルトのキーでの認証しか試行できないため、試行が失敗してパニック状態になります。パニック状態が発生した場合に自動的にリブートするように設定されているストレージシステムはブートループに入り、SEDでの認証が連続して失敗します。

設計上、このような状況でストレージシステムを停止するのは、認証の連続失敗回数の上限を超えたためにSEDが永続的にロックされた場合に、ストレージシステムがブートループに入ったり、意図しないデータ損失が発生したりするのを防ぐためです。ロックアウト保護の制限とタイプは、SEDの製造仕様とタイプによって異なります。

SEDタイプ	ロックアウトされるまでの認証の連続失敗回数	安全制限に達したときのロックアウト保護タイプ
HDD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンがNA00またはNA01のX440_PHM2800MCTO 800GB NSE SSD	5	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンがNA00またはNA01のX577_PHM2800MCTO 800GB NSE SSD	5	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンが上位のX440_PHM2800MCTO 800GB NSE SSD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンが上位のX577_PHM2800MCTO 800GB NSE SSD	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
その他すべての SSD モデル	1024	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。

すべての SED タイプでは、認証が成功すると試行回数が 0 にリセットされます。

ストレージシステムが指定されたどのキー管理サーバにもアクセスできないために停止した場合は、引き続きストレージシステムのブートを試行する前に、通信エラーの原因を特定して修正しておく必要があります。

暗号化をデフォルトで無効にする

ONTAP 9 .7以降では、Volume Encryption（VE）ライセンスがあり、オンボードまたは外部のキー管理ツールを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。必要に応じて、暗号化をデフォルトでクラスタ全体で無効にすることができます。

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か、クラスタ管理者から権限を委譲されたSVM管理者である必要があります。

ステップ

1. ONTAP 9 .7以降でクラスタ全体の暗号化をデフォルトで無効にするには、次のコマンドを実行します。

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。