NetAppボリューム暗号化の設定

ONTAP 9

NetApp
December 20, 2024

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

目次

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。

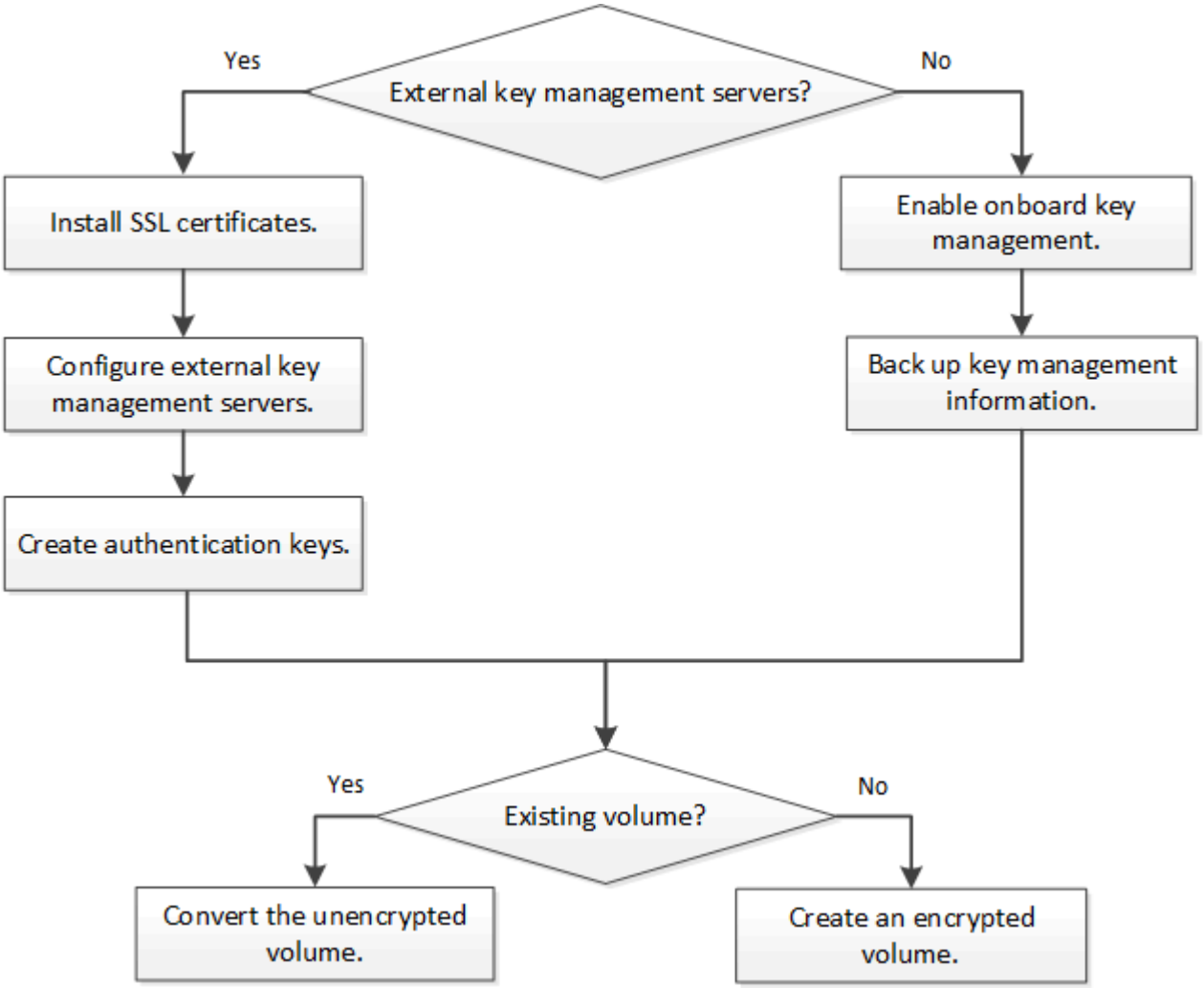
7-Modeからの移行	7-Mode Transition Tool 3.3以降では、7-Mode Transition Tool CLIを使用して、クラスタ システムのNVE対応デスティネーション ボリュームへのコピーベースの移行を実行できます。

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
000000000000000002000000000000100 8C07CC0AF1EF49E0105300EFC83004BF NSE-AK

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

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。