NetAppボリュームとアグリゲートの暗号化を設定する

ONTAP 9

NetApp
February 12, 2026

目次

NetAppボリュームとアグリゲートの暗号化を設定する

ONTAP NetAppボリュームとアグリゲートの暗号化について学ぶ

NetApp Volume Encryption（NVE）は、一度に1ボリュームずつ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、基盤のデバイスの転用、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を含む）の両方が暗号化されます。データへのアクセスは、ボリュームごとに1つずつ、固有のXTS-AES-256キーによって提供されます。外部のキー管理サーバーまたはOnboard Key Manager（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 システムで設定することを推奨します。
- オンボード キー マネージャは組み込みのツールで、データと同じストレージ システムからノードにキーを提供します。

ONTAP 9.7以降では、ボリューム暗号化（VE）ライセンスがあり、オンボードまたは外部の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っています。VEライセンスは"ONTAP One"に含まれています。外部またはオンボードのキーマネージャを設定すると、新しいアグリゲートと新しいボリュームの保存データの暗号化の設定方法が変わります。新しいアグリゲートでは、NetApp Aggregate Encryption（NAE）がデフォルトで有効になります。NAEアグリゲートの一部ではない新しいボリュームでは、NetApp Volume Encryption（NVE）がデフォルトで有効になります。データStorage Virtual Machine（SVM）にマルチテナントキー管理を使用する独自のキーマネージャ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は自動的にNVEで設定されます。

新規ボリュームまたは既存ボリュームで暗号化を有効にすることができます。NVEは、重複排除や圧縮を含む、ストレージ効率化機能をすべてサポートしています。ONTAP 9.14.1以降では、既存のSVMルートボリュームでNVEを有にする。

> SnapLockを使用している場合は、新しい空のSnapLockボリューム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、あらゆるタイプのアグリゲート（HDD、SSD、ハイブリッド、アレイLUN）、あらゆるRAIDタイプ、そしてONTAP Selectを含むサポートされているすべてのONTAP実装で使用できます。また、NVEをハードウェアベースの暗号化と組み合わせて使用することで、自己暗号化ドライブ上のデータを「二重暗号化」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保持されます。アグリゲート全体が削除されると、キーも削除されます。

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。

> `volume move`コマンドを使用して、NVEボリュームをNAEボリュームに変換したり、その逆を行ったりできます。NAEボリュームをNVEボリュームに複製することも可能です。

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

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。

- 連邦情報処理標準（FIPS）140-2またはOASIS KMIP標準に準拠した暗号化キー管理ソリューションが必要な場合。
- 暗号化キーを一元管理するマルチクラスタ ソリューションが必要な場合。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

外部キー管理のスコープ

外部キー管理のスコープによって、キー管理サーバの保護対象がクラスタ内の全SVMになるか、選択したSVMのみになるかが決まります。

- _クラスタスコープ_を使用すると、クラスタ内のすべてのSVMに対して外部キー管理を設定できます。クラスタ管理者は、サーバーに保存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スコープ_を使用して、クラスタ内の名前付きSVMの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SVMセット）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。特定のテナントのキーにアクセスできるのは、そのテナントのSVM管理者のみです。
    - ONTAP 9.17.1 以降では、Barbican KMSを使用してデータ SVM の NVE キーのみを保護できます。

- ONTAP 9.10.1以降では、Azure Key Vault と Google Cloud KMSを使用してデータSVMのNVEキーのみを保護できます。これは、9.12.0以降のAWS KMSで利用可能です。

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マネージャのリストは、"NetApp Interoperability Matrix Tool（IMT）"で入手できます。このリストは、IMTの検索機能に「キーマネージャ」と入力することで見つけることができます。

Azure Key VaultやAWS KMSなどのクラウドKMSプロバイダーはKMIPをサポートしていません。そのため、IMTには記載されていません。

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 マネージャを設定している場合、新しく作成したアグリゲートおよびボリュームはデフォルトで暗号化されます。暗号化せずに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 テキストの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ない。
	• キー マネージャが設定されていない。
	• プラットフォームまたはソフトウェアで暗号化がサポートされていない。
	• ハードウェア暗号化が有効になっている。

ONTAP	すべてのONTAP実装。Cloud Volumes ONTAPのサポートは、ONTAP 9.5以降で利用できます。
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上のデータは暗号化できません。ONTAP 9.14.1より前のバージョンでは、SVMルートボリューム上のデータをNVEで暗号化することはできません。ONTAP 9.14.1以降、ONTAPはSVMルートボリュームのNVEをサポートしています。
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	MetroClusterはONTAP 9.8以降でサポートされます。 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。
ストレージ効率	重複排除、圧縮、コンパクション、FlexClone。 クローンは、親からクローンを分割した後でも、親と同じキーを使用します。分割されたクローンに対して `volume move`を実行する必要があります。これにより、分割されたクローンのキーは異なります。
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。暗号化はソースに設定してデスティネーションには設定しないことも、その逆も可能です。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の両方で手動で設定する必要があります。NVEの設定およびNVEによるボリューム データの暗号化を参照してください。 • 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	SnapLockは、コンプライアンスモードとエンタープライズモードの両方でサポートされていますが、新規ボリュームのみが対象となります。既存のSnapLockボリュームでは暗号化を有効にできません。

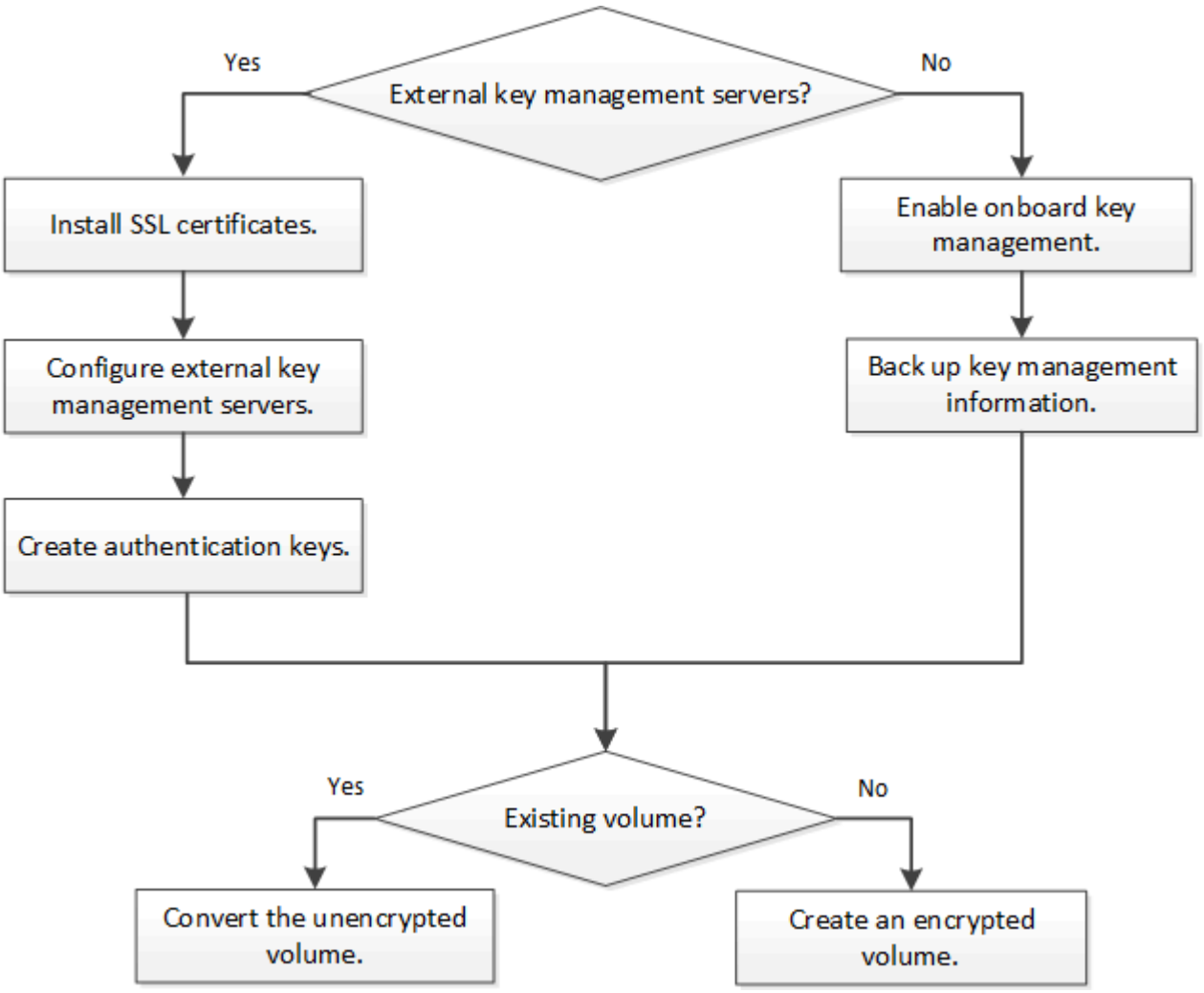
FlexGroupボリューム	FlexGroupボリュームはサポートされています。デスティネーションアグリゲートは、ボリュームレベルまたはアグリゲートレベルのいずれかで、ソースアグリゲートと同じタイプである必要があります。ONTAP 9.5以降では、FlexGroupボリュームのインプレースキー再生成がサポートされています。
7-Modeからの移行	7-Mode Transition Tool 3.3以降では、7-Mode Transition Tool CLIを使用して、クラスタ システムのNVE対応デスティネーション ボリュームへのコピーベースの移行を実行できます。

関連情報

- "FAQ - NetApp ボリューム暗号化とNetApp アグリゲート暗号化"
- "storage aggregate create"

ONTAP NetApp Volume Encryption 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

する必要があります。ライセンスをインストールする前に、"ONTAP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。

NVEの設定

ONTAPクラスタバージョンがNVEをサポートしているかどうかを確認する

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。 `version`コマンドを使用して、クラスタのバージョンを確認できます。

タスク概要

クラスタ 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。

手順

1. クラスタ 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
   ```

   コマンド出力にテキスト `1Ono-DARE`（「保存データの暗号化なし」）が表示される場合、または"サポートの詳細"に記載されていないプラットフォームを使用している場合、NVEはサポートされません。

ONTAPクラスタにボリューム暗号化ライセンスをインストールする

VEライセンスを取得すると、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。NVEでデータを暗号化するには、このライセンスが必要です。"ONTAP One"に含まれています。

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。暗号化バンドルは現在提供されていませんが、引き続き有効です。現在必須ではありませんが、既存のお客様は"ONTAP Oneにアップグレード"を選択できます。

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。
- 営業担当から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"。

   VE ライセンスパッケージ名は `VE`です。

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します。"。

外部キー管理の設定

ONTAP NetApp Volume Encryptionを使用した外部キー管理の設定について学習します

クラスタが暗号化されたデータにアクセスするために使用する鍵を保護するために、1台以上の外部鍵管理サーバを使用できます。外部鍵管理サーバとは、ストレージ環境内のサードパーティ製システムであり、Key Management Interoperability Protocol（KMIP）を使用してノードに鍵を提供します。ONTAPは、オンボードキーマネージャに加えて、複数の外部鍵管理サーバをサポートしています。

ONTAP 9.10.1以降では、Azure Key Vault または Google Cloud Key Manager Serviceを使用してデータSVMのNVEキーを保護できます。ONTAP 9.11.1以降では、クラスタ内に複数の外部キーマネージャを設定できます。クラスタ化されたキーサーバを設定するを参照してください。ONTAP 9.12.0以降では、"AWSのKMS"を使用してデータSVMのNVEキーを保護できます。ONTAP 9.17.1以降では、OpenStackのBarbican KMSを使用してデータSVMのNVEキーを保護できます。

ONTAP System Managerで外部キーマネージャを管理する

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保存、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保存、管理することもできます。

オンボード キー マネージャを使用する場合、キーはクラスタ内部のセキュアなデータベースで格納、管理されます。スコープはクラスタです。外部キー管理ツールを使用する場合、キーはクラスタの外部で格納、管理されます。スコープは、クラスタでもStorage VMでもあり得ます。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、Storage VMと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 サーバには、最大3台のセカンダリ キー サーバを追加してクラスタ化できます。

外部キー管理ツールの設定

ストレージVMに外部キーマネージャーを追加するには、ストレージVMのネットワークインターフェースを構成する際に、オプションのゲートウェイを追加する必要があります。ストレージVMがネットワークルートなしで作成された場合は、外部キーマネージャー用のルートを明示的に作成する必要があります。"LIF（ネットワーク インターフェイス）の作成"を参照してください。

手順

外部キー管理ツールの設定は、System Manager内の複数のメニューから開始できます。

1. 次のいずれかのオプションを使用して、外部キー管理の設定を開始します。

ワークフロー	ナビゲーション	開始ステップ

Key Managerを設定する	クラスター > 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ー*を選択します。
ローカル階層を追加	ストレージ > 階層	*+ ローカル層の追加*を選択します。「キーマネージャーの設定」チェックボックスをオンにします。*外部キーマネージャー*を選択します。
ストレージを準備	ダッシュボード	*容量*セクションで*ストレージの準備*を選択します。次に、「キーマネージャーの設定」を選択します。*外部キーマネージャー*を選択します。
暗号化を設定する（ストレージ VM スコープのキー マネージャのみ）	ストレージ > **Storage VM**	ストレージVMを選択します。*設定*タブを選択します。*セキュリティ*の*暗号化*セクションで、⚙を選択します。

2. プライマリ キー サーバーを追加するには、＋ Add を選択し、**IP Address or Host Name** および **Port** フィールドに入力します。
3. 既にインストールされている証明書は、「**KMIP** サーバー **CA** 証明書」および「**KMIP** クライアント証明書」フィールドに表示されます。以下のいずれかの操作を実行できます：
   - ⌄を選択して、キー マネージャーにマップするインストール済みの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、クライアント証明書は 1 つだけ選択できます。）
   - まだインストールされていない証明書を追加し、外部キー マネージャーにマップするには、*新しい証明書の追加*を選択します。
   - 外部キー マネージャーにマップ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 サーバーを追加するには、*セカンダリ キー サーバー*列で*追加*を選択し、詳細を入力します。
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の編集

すでに外部キー管理ツールの設定が完了している場合は、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、次のいずれかの手順を実行します。

Scope	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 マネージャ	クラスター > 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、*外部キーマネージャーの編集*を選択します。

Storage VMスコープ外部キー マネージャ	ストレージ > **Storage VM**	ストレージVMを選択します。*設定*タブを選択します。*セキュリティ*の*暗号化*セクションで、⋮を選択し、*外部キーマネージャーの編集*を選択します。

2. 既存の鍵サーバーは*鍵サーバー*テーブルにリストされます。以下の操作を実行できます：
   - ＋ Add を選択して新しいキー サーバーを追加します。
   - キーサーバーを削除するには、キーサーバー名を含むテーブルセルの末尾にある⋮を選択します。そのプライマリキーサーバーに関連付けられているセカンダリキーサーバーも設定から削除されます。

外部キー管理ツールの削除

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. 次のいずれかの手順を実行して、外部キー管理を削除します。

Scope	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 マネージャ	クラスター > 設定	*Security*セクションまでスクロールします。*Encryption*で⋮を選択し、*Delete External Key Manager*を選択します。
Storage VMスコープ外部キー マネージャ	ストレージ > **Storage VM**	ストレージVMを選択します。*設定*タブを選択します。*セキュリティ*の*暗号化*セクションで、⋮を選択し、*外部キーマネージャーの削除*を選択します。

キー管理ツール間のキーの移行

クラスタで複数のキー管理ツールが有効になっている場合、1つのキー管理ツールから別のキー管理ツールにキーを移行する必要があります。このプロセスは、System Managerで自動的に実行されます。

- オンボード キー マネージャまたは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て、一部のボリュームが暗号化されている場合、Storage VMレベルで外部キー管理ツールを設定する際には、クラスタレベルのオンボード キー マネージャまたは外部キー管理ツールからStorage VMレベルの外部キー管理ツールにキーを移行する必要があります。このプロセスは、System Managerで自動的に実行されます。
- 暗号化せずにStorage VMにボリュームを作成した場合、キーを移行する必要はありません。

ONTAPクラスタに**SSL**証明書をインストールする

クラスタとKMIPサーバの間では、相互のIDを検証してSSL接続を確立するためにKMIP SSL証明書を使用します。KMIPサーバとのSSL接続を設定する前に、クラスタのKMIPクライアントSSL証明書、およびKMIPサーバのルートCertificate Authority（CA;認証局）のSSLパブリック証明書をインストールする必要があります。

タスク概要

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

開始する前に

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

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

手順

1. クラスタにSSL KMIPクライアント証明書をインストールします。

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

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

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

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

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

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

関連情報

- "security certificate install"

ONTAP 9.6以降で**NVE**の外部キー管理を有効にする

KMIPサーバを使用して、クラスタが暗号化データにアクセスするために使用するキーを保護します。ONTAP 9.6以降では、データSVMが暗号化データにアクセスするために使用するキーを保護するために、別の外部キーマネージャを設定できるようになりました。

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

タスク概要

クラスタまたはSVMには最大4台のKMIPサーバーを接続できます。冗長性と災害復旧のために、少なくとも2

台のサーバーを使用してください。

外部キー管理のスコープによって、キー管理サーバの保護対象がクラスタ内の全SVMになるか、選択したSVMのみになるかが決まります。

- _クラスタスコープ_を使用すると、クラスタ内のすべてのSVMに対して外部キー管理を設定できます。クラスタ管理者は、サーバーに保存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スコープ_を使用して、クラスタ内のデータSVMの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SVMセット）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。特定のテナントのキーにアクセスできるのは、そのテナントのSVM管理者のみです。
- 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>
  ```

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

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でき、外部キー管理はSVMスコープで設定できます。`security key-manager key migrate`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マネージャにキーを移行できます。

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

開始する前に

- KMIP SSLクライアント証明書とサーバ証明書をインストールしておく必要があります。
- KMIP サーバーは、各ノードのノード管理 LIF からアクセスできる必要があります。
- このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。
- MetroCluster環境内：
  - 外部キー管理を有効にする前に、MetroCluster を完全に構成する必要があります。
  - 両方のクラスタに同じ KMIP SSL 証明書をインストールする必要があります。
  - 両方のクラスタで外部キーマネージャを設定する必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   ```

```
host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

> `security key-manager external enable`コマンドは、 `security key-manager setup`コマンドに代わるものです。クラスタログインプロンプトでコマンドを実行すると、 `*admin_SVM*`はデフォルトで現在のクラスタの管理SVMになります。 `security key-manager external modify`コマンドを実行して、外部キー管理の設定を変更できます。

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

```
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の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
```

> - SVMログインプロンプトでコマンドを実行すると、 `SVM`デフォルトで現在のSVMが選択されます。 `security key-manager external modify`コマンドを実行して、外部キー管理設定を変更できます。
> - 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 `security key-manager external enable`コマンドを繰り返す必要はありません。

次のコマンドは、デフォルトのポート5696でリッスンする単一のキーサーバーで `svm1`の外部キー管理を有効にします：

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

3. 最後の手順をその他のSVMに対して繰り返します。

`security key-manager external add-servers`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`コマンドは `security key-manager add`コマンドに代わるものです。link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-add-servers.html["ONTAPコマンド リファレンス"^]で `security key-manager external add-servers`の詳細をご覧ください。

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

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

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      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されたボリュームに変換します。

   ```
   volume encryption conversion start
   ```

   ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。

関連情報

- クラスタ化された外部キー サーバの設定
- "system license add"
- "セキュリティキー・マネージャーキーの移行"
- "セキュリティ key-manager external add-servers"
- "security key-manager external show-status"

ONTAP 9.5以前で**NVE**の外部キー管理を有効にする

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

タスク概要

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

開始する前に

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

手順

1. クラスタ ノードのキー管理ツールの接続を設定します。

   ```
   security key-manager setup
   ```

   キー管理ツールのセットアップが開始されます。

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

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

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

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

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

4. 冗長性を確保するためにKMIPサーバをもう1つ追加します。

   `security key-manager add -address key_management_server_ipaddress`

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

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

5. 設定したすべてのKMIPサーバが接続されていることを確認します。

   `security key-manager show -status`

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

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

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

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

   `volume encryption conversion start`

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

クラウド プロバイダを使用した**ONTAP** データ**SVM**の**NVE**キーの管理

ONTAP 9.10.1以降では、"Azure Key Vault（AKV）"と"Google Cloud Platform の Key Management Service（Cloud KMS）"を使用して、クラウドホスト型アプリケーションでONTAP暗号化キーを保護できます。ONTAP 9.12.0以降では、"AWSのKMS"を使用してNVEキーを保護することもできます。

AWS KMS、AKV、Cloud KMS は、データ SVM の"NetApp Volume Encryption（NVE）キー"の保護にのみ使用できます。

タスク概要

クラウド プロバイダによるキー管理は、CLIまたはONTAP REST APIを使用して有効にすることができます。

クラウド プロバイダを使用してキーを保護する場合、クラウドキー管理エンドポイントとの通信にはデフォルトでデータSVM LIFが使用されることに注意してください。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）との通信にはノード管理ネットワークが使用されます。クラスタ ネットワークが正しく設定されていない場合、クラスタはキー管理サービスを適切に使用できません。

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 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。代わりに"外部KMIP"を使用できます。
- クラウド プロバイダによるキー管理は、MetroCluster構成では利用できません。
- クラウド プロバイダによるキー管理を設定できるのは、データSVMのみです。

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。
- "ボリューム暗号化（VE）ライセンスとマルチテナント暗号化キー管理（MTEKM）ライセンスがインストールされている必要があります。"。これらのライセンスは"ONTAP One"に含まれています。
- 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キーに対応するグラント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、"助成金"のAWSドキュメントを参照してください。

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 キーを取得しておきます。
2. 権限レベルを advanced に設定します： `set -priv advanced`
3. AWS KMS を有効にする： `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 が正しく設定されていることを確認します： `security key-manager external aws show -vserver` *`svm_name`*

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

Azure

ONTAP SVMでAzure Key Vaultを有効にする

1. 始める前に、Azureアカウントから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）を取得する必要があります。また、クラスター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。これは次のコマンドで確認できます `cluster show`。 `cluster show`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。
2. 権限レベルを advanced に設定します `set -priv advanced`
3. SVM で AKV を有効にします。 `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、Azure アカウントのクライアント証明書またはクライアント シークレットを入力します。
4. AKV が正しく有効化され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正常でない場合は、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。

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

Google Cloud

ONTAP SVMでCloud KMSを有効にする

1. 始める前に、Google Cloud KMSアカウントキーファイルの秘密鍵をJSON形式で取得してください。これはGCPアカウントで確認できます。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。これはコマンド `cluster show`で確認できます。 `cluster show`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。
2. 特権レベルを詳細に設定します： `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、Service Account Private Keyを含むJSONファイルの内容を入力します
4. Cloud KMS が正しいパラメータで設定されていることを確認してください： `security key-manager external gcp show vserver *svm_name*` `kms_wrapped_key_status`のステータスは、暗号化されたボリュームが作成されていない場合、 `"UNKNOWN"`になります。サービス到達可能性が OK でない場合は、データ SVM LIF を介して GCP 鍵管理サービスへの接続を確立してください。

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

データSVMに1つ以上の暗号化ボリュームがすでに設定されており、対応するNVEキーが管理SVMのオンボードキーマネージャによって管理されている場合は、それらのキーを外部キー管理サービスに移行する必要があります。CLIでこれを行うには、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に新しい暗号化ボリュームを作成することはできません。

関連情報

- "Cloud Volumes ONTAP の NetApp 暗号化ソリューションによるボリュームの暗号化"
- "セキュリティ キーマネージャー外部"

Barbican KMSでONTAPキーを管理する

ONTAP 9.17.1以降では、OpenStackの"Barbican KMS"を使用してONTAP暗号化キーを保護できます。Barbican KMSは、キーを安全に保存およびアクセスするためのサービスです。Barbican KMSは、データSVMのNetApp Volume Encryption（NVE）キーを保護するために使用できます。Barbicanは、OpenStackのIDサービスである"OpenStack

Keystone"を認証に使用します。

タスク概要

Barbican KMSによるキー管理は、CLIまたはONTAP REST APIで設定できます。9.17.1リリースでは、Barbican KMSのサポートに以下の制限があります：

- Barbican KMSは、NetApp Storage Encryption（NSE）およびNetApp Aggregate Encryption（NAE）ではサポートされていません。代わりに、NSEおよびNVEキーには"外部KMIP"または"オンボード キー マネージャー（OKM）"を使用できます。
- Barbican KMS は MetroCluster 構成ではサポートされていません。
- Barbican KMS はデータ SVM に対してのみ設定できます。管理 SVM では使用できません。

特に明記されていない限り、 `admin`権限レベルの管理者は次の手順を実行できます。

開始する前に

- Barbican KMSとOpenStack Keystoneを設定する必要があります。Barbicanで使用しているSVMは、BarbicanおよびOpenStack Keystoneサーバーへのネットワーク アクセスが必要です。
- Barbican サーバーおよびOpenStack Keystone サーバーにカスタム証明機関（CA）を使用している場合は、 `security certificate install -type server-ca -vserver <admin_svm>`を使用して CA 証明書をインストールする必要があります。

Barbican KMS 構成を作成してアクティブ化する

SVM に新しい Barbican KMS 構成を作成し、アクティブ化することができます。SVM には複数の非アクティブな Barbican KMS 構成を含めることができますが、アクティブ化できるのは一度に 1 つだけです。

手順

1. SVM の新しい非アクティブな Barbican KMS 構成を作成します：

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id`は、Barbican鍵暗号化キー（KEK）の鍵識別子です。 `https://`を含む完全なURLを入力してください。

> 一部のURLには疑問符（?）が含まれています。疑問符はONTAPコマンドラインのアクティブヘルプを起動します。疑問符を含むURLを入力するには、まずコマンド `set -active-help false`でアクティブヘルプを無効にする必要があります。アクティブヘルプは、後でコマンド `set -active-help true`で再度有効にすることができます。詳細については、"ONTAPコマンド リファレンス"をご覧ください。

   - `-keystone-url`は、OpenStack Keystone認証ホストのURLです。 `https://`を含む完全なURLを入力してください。
   - `-application-cred-id` はアプリケーション認証クレデンシャル ID です。

このコマンドを入力すると、アプリケーション認証クレデンシャルの秘密キーの入力を求められます。このコマンドは、非アクティブなBarbican KMS構成を作成します。

次の例では、SVM `svm1`用に `config1`という名前の新しい非アクティブなBarbican KMS構成を作成します：

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. 新しい Barbican KMS 構成をアクティブ化します：

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

このコマンドを使用すると、Barbican KMS 構成を切り替えることができます。SVM 上に既にアクティブな Barbican KMS 構成がある場合は、その構成は非アクティブになり、新しい構成がアクティブになります。

3. 新しい Barbican KMS 構成がアクティブであることを確認します：

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

このコマンドは、SVMまたはノード上のアクティブなBarbican KMS構成のステータスを表示します。例えば、ノード `node1`上のSVM `svm1`にアクティブなBarbican KMS構成がある場合、次のコマンドはその構成のステータスを返します：

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Barbican KMS構成の認証クレデンシャルと設定を更新する

アクティブまたは非アクティブな Barbican KMS 構成の現在の設定を表示および更新できます。

手順

1. SVM の現在の Barbican KMS 構成を表示します：

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

SVM 上の各 Barbican KMS 構成のキー ID、OpenStack Keystone URL、アプリケーション認証クレデンシャル ID が表示されます。

2. Barbican KMS 構成の設定を更新します：

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

このコマンドは、指定されたBarbican KMS構成のタイムアウトと検証設定を更新します。 `timeout`ONTAPがBarbicanからの応答を待機する時間を秒単位で指定します。この時間を超えると接続が失敗します。デフォルト `timeout`は10秒です。 `verify`および `verify-host`は、接続前にBarbicanホストのIDとホスト名をそれぞれ検証するかどうかを指定します。デフォルトでは、これらのパラメータは `true`に設定されています。 `vserver`および `config-name`パラメータは必須です。その他のパラメータはオプションです。

3. 必要に応じて、アクティブまたは非アクティブな Barbican KMS 構成の認証クレデンシャルを更新します。

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

このコマンドを入力すると、新しいアプリケーション認証クレデンシャルの秘密キーの入力を求められます。

4. 必要に応じて、アクティブな Barbican KMS 構成の不足している SVM キー暗号化キー（KEK）を復元します：

   a. 失われた SVM KEK を次のように復元します： `security key-manager external barbican restore`

```
security key-manager external barbican restore -vserver <svm_name>
```

このコマンドは、Barbican サーバーと通信して、アクティブな Barbican KMS 構成の SVM KEK を復元します。

5. 必要に応じて、Barbican KMS 構成の SVM KEK のキーを再設定します：

   a. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

   b. SVM KEK を次のように再キー化します： `security key-manager external barbican rekey-internal`

   ```
   security key-manager external barbican rekey-internal -vserver
   <svm_name>
   ```

   このコマンドは、指定されたSVMの新しいSVM KEKを生成し、ボリューム暗号化キーを新しいSVM KEKで再ラップします。新しいSVM KEKは、アクティブなBarbican KMS構成によって保護されます。

Barbican KMS と Onboard Key Manager 間で暗号化キーを移行する

Barbican KMSからOnboard Key Manager（OKM）へ、またその逆の方法で暗号化キーを移行できます。OKMの詳細については、"オンボード キー管理の有効化（ONTAP 9.6以降）"をご覧ください。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 必要に応じて、Barbican KMS から OKM にキーを移行します：

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

   `svm_name`は、Barbican KMS 構成を持つ SVM の名前です。

3. 必要に応じて、OKM から Barbican KMS に暗号化キーを移行します：

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

Barbican KMS 構成を無効化して削除する

暗号化されたボリュームのないアクティブな Barbican KMS 構成を無効にすることができ、非アクティブな Barbican KMS 構成を削除することができます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. アクティブな Barbican KMS 構成を無効にします：

```
security key-manager keystore disable -vserver <svm_name>
```

SVM 上に NVE で暗号化されたボリュームが存在する場合は、Barbican KMS 構成を無効にする前に、それらを復号化するキーを移行する必要があります。新しい Barbican KMS 構成をアクティブ化する場合、NVE ボリュームの復号化やキーの移行は不要で、現在アクティブな Barbican KMS 構成が無効になります。

3. 非アクティブな Barbican KMS 構成を削除します：

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

ONTAP 9.6以降でNVEの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際にクラスタで使用するキーを安全に保管できます。オンボード キー マネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスク概要

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

MetroCluster構成がある場合は、まずローカルクラスタで `security key-manager onboard enable`コマンドを実行し、次にリモートクラスタで `security key-manager onboard sync`コマンドを実行する必要があります。その際、各クラスタで同じパスフレーズを使用してください。ローカルクラスタで `security key-manager onboard enable`コマンドを実行し、その後リモートクラスタで同期する場合は、リモートクラスタで `enable`コマンドを再度実行する必要はありません。

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

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

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

ONTAP保存データ暗号化を設定する場合、Commercial Solutions for Classified（CSfC）の要件を満たすには、NSEとNVEを使用し、オンボードキーマネージャがCommon Criteriaモードで有効になっていることを確認する必要があります。"CSfC解決策概要"を参照してください。

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

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

  クラスタパスフレーズの入力に5回失敗した場合は、24時間待つか、ノードをリブートして制限をリセットします。

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

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

オンボードキーマネージャーは、キーを揮発性メモリに保存します。揮発性メモリの内容は、システムの再起動または停止時に消去されます。システムは停止後、30秒以内に揮発性メモリを消去します。

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。
- 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
```

`cc-mode-enabled=yes`を設定して、再起動後にユーザーが認証キーマネージャーのパスフレーズを入力するように要求します。NVEの場合、 `cc-mode-enabled=yes`を設定すると、 `volume create`コマンドと `volume move start`コマンドで作成したボリュームが自動的に暗号化されます。 `- cc-mode-enabled`オプションはMetroCluster構成ではサポートされていません。 `security key-manager onboard enable`コマンドは `security key-manager setup`コマンドに置き換えられます。

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

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

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 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 `security key-manager query key`コマンドに置き換わります。

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

5. オプションで、プレーンテキストボリュームを暗号化されたボリュームに変換できます。

   ```
   volume encryption conversion start
   ```

   ボリュームを変換する前に、オンボード キー マネージャの設定を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。

終了後の操作

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

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

関連情報

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

ONTAP 9.5以前でNVEの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際にクラスタで使用するキーを安全に保管できます。オンボード キー マネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

タスク概要

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

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

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

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

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

パスフレーズの試行が失敗した場合は、ノードを再起動する必要があります。

開始する前に

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

  "外部キー管理からオンボード キー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- Onboard Key Managerを設定する前に、MetroCluster環境を設定します。

手順

1. キー管理ツールのセットアップを開始します。

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

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

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

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

...

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

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

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

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

   `security key-manager show-key-store`

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

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

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

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

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

   ```
   volume encryption conversion start
   ```

   ボリュームを変換する前に、オンボードキーマネージャーを設定してください。MetroCluster環境では、両方のサイトで設定してください。

終了後の操作

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

オンボードキーマネージャのパスフレーズを設定する際は、災害発生時に備えて、ストレージシステム外部の安全な場所に情報をバックアップしてください。"オンボード キー管理情報の手動バックアップ"を参照してください。

関連情報

- "オンボード キー管理情報の手動バックアップ"
- "外部キー管理からオンボード キー管理への移行"
- "security key-manager show-key-store"

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

> ONTAP 9.6 以降では、クラスタにノードを追加するたびに `security key-manager onboard sync`コマンドを実行する必要があります。
>
> ONTAP 9.5 以前では、クラスタにノードを追加するたびに `security key-manager setup`コマンドを実行する必要があります。
>
> オンボードキー管理を使用してクラスタにノードを追加する場合は、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構成を使用する場合は、次のガイドラインを確認してください。

- ONTAP 9.6以降では、最初にローカルクラスタで `security key-manager onboard enable`を実行し、次にリモートクラスタで `security key-manager onboard sync`を実行する必要があります。それぞれで同じパスフレーズを使用してください。

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

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

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

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

パスフレーズの入力が失敗した場合は、ノードを再起動してください。再起動後、パスフレーズを再度入力してください。

関連情報

- "クラスターイメージコマンド"
- "セキュリティキー・マネージャ外部有効化"
- "セキュリティキー・マネージャーオンボード有効化"

NVE または NAE を使用してボリューム データを暗号化する

NVEを使用したONTAPボリュームデータの暗号化について学ぶ

ONTAP 9.7以降では、NVE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以前のバージョンでは、新しいボリュームおよび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には、VEライセンスをインストールして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。

ONTAPでVEライセンスを使用した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"とオンボードまたは外部キー管理を使用している場合、新規に作成され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。

タスク概要

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（NetApp Aggregate Encryptionの略）と呼ばれます。NAEアグリゲート内のすべてのボリュームは、NAE暗号化または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。このデフォルトを上書きして、NVE暗号化を使用するように設定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 ボリュームが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でNAEアグリゲートを作成する	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
非NAE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アグリゲートを非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 false`

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

次のコマンドは、 `aggr1`の集約レベルの暗号化を有効にします：

- 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
```

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

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

   次のコマンドは`aggr1`が暗号化に対して有効になっていることを確認します：

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

`storage aggregate show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-show.html?q=storage+aggregate+show["ONTAPコマンド リファレンス"^]をご覧ください。

終了後の操作

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

KMIP サーバーを使用してノードの暗号化キーを保存している場合、ボリュームを暗号化すると、ONTAP は自動的に暗号化キーをサーバーに「プッシュ」します。

ONTAPで新しいボリュームの暗号化を有効にする

`volume create`コマンドを使用して、新しいボリュームで暗号化を有効にすることができます。

タスク概要

NetApp ボリューム暗号化（NVE）と、ONTAP 9.6以降ではNetApp アグリゲート暗号化（NAE）を使用してボリュームを暗号化できます。NAEとNVEの詳細については、ボリューム暗号化の概要を参照してください。

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

新しいボリュームの暗号化を有効にする手順は、使用しているONTAPのバージョンと環境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 `cc-mode`を有効にすると、 `-encrypt true`を指定したかどうかに関係なく、 `volume create`コマンドで作成したボリュームが自動的に暗号化されます。
- ONTAP 9.6以前のリリースでは、暗号化を有効にするには `-encrypt true`と `volume create`コマンドを使用する必要があります（ `cc-mode`を有効にしていない場合）。
- ONTAP 9.6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。このタスクの詳細については、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を参照してください。
- ONTAP 9.7以降では、"VEライセンス"とオンボードまたは外部キー管理を使用している場合、新規作成されたボリュームはデフォルトで暗号化されます。デフォルトでは、NAEアグリゲートに作成される新規ボリュームは、NVEではなくNAEタイプになります。
  - ONTAP 9.7以降のリリースでは、NAEアグリゲートにボリュームを作成する `volume create`コマンドに `-encrypt true`を追加すると、そのボリュームはNAEではなくNVE暗号化されます。NAEアグリゲート内のすべてのボリュームは、NVEまたはNAEのいずれか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 ボリュームが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。

作成するには...	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がサポートされていないONTAP 9.6以前では、 `-encrypt true`ボリュームをNVEで暗号化することを指定します。ボリュームがNAEアグリゲート内に作成されるONTAP 9.7以降では、 `-encrypt true`NAEのデフォルトの暗号化タイプをオーバーライドして、代わりにNVEボリュームを作成します。
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`

`volume create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-create.html["ONTAPコマンド リファレンス"^]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
```

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

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暗号化キーがサーバに自動的に「プッシュ」されます。

既存のONTAPボリュームでNAEまたはNVE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、 `volume move start`コマンドまたは `volume encryption conversion start`コマンドのいずれかを使用できます。

タスク概要

`volume encryption conversion start`コマンドを使用すると、ボリュームを別の場所に移動することなく、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。または、 `volume move start`コマンドを使用することもできます。

volume encryption conversion startコマンドを使用した既存のボリュームに対する暗号化の有効化

`volume encryption conversion start`コマンドを使用すると、ボリュームを別の場所に移動しなくても、既存のボリュームの暗号化を「その場で」有効にすることができます。

変換操作を開始したら、必ず完了させてください。操作中にパフォーマンスの問題が発生した場合は、 `volume encryption conversion pause` コマンドを実行して操作を一時停止し、 `volume encryption conversion resume` コマンドを実行して操作を再開することができます。

`volume encryption conversion start`を使用してSnapLockボリュームを変換することはできません。

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
```

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

次のコマンドは、既存のボリューム `vol1`の暗号化を有効にします：

```
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`

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

   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`

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

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

```
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

KMIP サーバーを使用してノードの暗号化キーを保存している場合、ボリュームを暗号化すると、ONTAP は自動的に暗号化キーをサーバーに「プッシュ」します。

volume move startコマンドを使用した既存のボリュームに対する暗号化の有効化

`volume move start`コマンドを使用して、既存のボリュームを移動することで暗号化を有効にすることができます。同じアグリゲートを使用することも、別のアグリゲートを使用することもできます。

タスク概要

- ONTAP 9.8以降では、 `volume move start`を使用してSnapLockまたはFlexGroupボリュームの暗号化を有効にすることができます。
- 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、`volume move start`コマンドで作成したボリュームは自動的に暗号化されます。 `-encrypt-destination true`を指定する必要はありません。
- 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（NetAppボリューム暗号化を使用していることを意味します）と呼ばれます。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アグリゲート暗号化の略）と呼ばれます。プレーンテキストボリュームはNAEアグリゲートではサポートされていません。
- ONTAP 9.14.1以降では、SVMルートボリュームをNVEで暗号化できます。詳細については、SVMルートボリュームでのNetApp Volume Encryptionの設定を参照してください。

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。

変換するには...	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`

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

次のコマンドは、`vol1`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ます：

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

宛先でアグリゲートレベルの暗号化が有効になっていると仮定すると、次のコマンドは、`vol1`という名前の NVE 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、`vol2`という名前の NAE ボリュームを NVE ボリュームに変換します：

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

次のコマンドは、`vol2`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、 `vol2`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ます：

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

2. クラスタの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。

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

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

```
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`

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

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

```
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は、ボリュームを暗号化すると暗号化キーがサーバに自動的にプッシュされます。

ONTAP SVMルートボリュームにNVEを設定する

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）を有効にできます。NVEを使用すると、ルート ボリュームが一意のキーで暗号化されるため、SVMのセキュリティが強化されます。

タスク概要

SVMルート ボリュームでのNVEは、SVMの作成後にのみ有効にできます。

開始する前に

- SVMルート ボリュームは、NetApp Aggregate Encryption（NAE）で暗号化されたアグリゲートに配置しないでください。
- オンボード キー マネージャや外部キー 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か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

SVMルート ボリュームでNVEを有効にする方法は、インプレースで行う方法と、アグリゲート間でボリュームを移動する方法があります。

ルート ボリュームをインプレースで暗号化する

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。 `volume show -encryption-type volume`には、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 ボリュームを移動して暗号化する

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
   ```

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

2. `volume move`操作が `volume move show`コマンドで成功したことを確認します。 `volume show -encryption-type volume`には、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を選択し、次に 編集 を選択します。
3. ストレージと最適化の見出しで、暗号化を有効にするを選択します。
4. 保存を選択します。

ONTAPノードのルートボリュームにNVEを構成する

ONTAP 9.8以降では、NetApp Volume Encryptionを使用してノードのルート ボリュームを保護できます。

タスク概要

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のルートボリュームには適用されません。SVMのルートボリュームは、アグリゲートレベルの暗号化によって保護できます。ONTAP 9.14.1以降、NVE

ルート ボリュームの暗号化は、いったん開始したら最後まで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 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たことを確認します。

   ```
   volume show -fields
   ```

   以下は、暗号化されたボリュームの出力例です。

   ```
   ::> 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

商標に関する情報